Configuring SNMP, BOOTP, DHCP, and RARP Services

Router Software Version 10.0
Site Manager Software Version 4.0

Software Version BNX 6.0
Site Manager Software Version BNX 6.0

Part No. 112923 Rev. A
January 1996

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. January 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, BCN, BLN, BN, CN, FRE, LN, Optivity, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and AN, ANH, ASN, BaySIS, BayStack, BCNX, BLNX, BNX, EZ Internetwork, EZ LAN, FN, PathMan, PhonePlus, PPX, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Software Suites xiii
Audience xiv
Bay Networks Customer Support xiv
CompuServe xv
InfoFACTS xvi
World Wide Web xvi
How to Get Help xvi
Conventions xvi
Ordering Bay Networks Publications xvii
Acronyms xviii

Chapter 1
Configuring SNMP Services

SNMP Overview 1-1
Remote Network Monitoring (RMON) 1-2
The RMON Groups 1-3
For More Information about SNMP 1-5
SNMP Implementation Notes 1-6
Internet Protocol (IP) 1-6
Thresholds 1-6
Threshold Example 1-7
Traps 1-9
RMON 1-9
RMON Interoperability Issues 1-10
RMON Memory Use 1-10
Interoperability Issues and Memory Use for RMON Groups 1-11
Enabling SNMP Services 1-16
Enabling IP on an Interface 1-16

Accessing SNMP Parameters 1-20
Editing SNMP Global Parameters 1-21
Editing SNMP Community Parameters 1-24
Adding an SNMP Community 1-24
Editing an SNMP Community 1-26
Deleting an SNMP Community 1-26
Configuring SNMP Community Members 1-27
Adding a Manager 1-27
Editing a Manager 1-29
Deleting a Manager 1-31
Editing Threshold Parameters 1-31
Configuring the Threshold Polling Interval 1-31
Configuring a Threshold 1-33
Editing Trap Parameters 1-40
Configuring Traps 1-40
Configuring Exceptions 1-41
Deleting Exceptions 1-44

Chapter 2
Configuring BOOTP Services

BOOTP Relay Agent Overview 2-1
Implementation Notes 2-5
Setting the Router Mode 2-5
Specifying a Forwarding Route for BOOTREQUEST Packets 2-5
Filtering BOOTP and DHCP Packets 2-5
Improving the Efficiency of Packet Relay 2-6
Specifying BOOTP Servers 2-6
Using Traffic Filters 2-6
Using Unnumbered Interfaces 2-7
Enabling BOOTP Services 2-7
Enabling BOOTP on an Interface 2-8
Accessing BOOTP Parameters 2-8
Editing BOOTP Relay Agent Parameters 2-9
Specifying Interfaces That Receive and Relay BOOTP Packets 2-11
Deleting an Input/Output Address Pair 2-15
Configuring an AN to Use EZ-Install over a Frame Relay PVC 2-15

Specifying Servers for BOOTP Services 2-17
Deleting the BOOTP Relay Agent from an IP Interface 2-22
Deleting BOOTP Globally 2-22

Chapter 3
Configuring DHCP Services

DHCP Overview 3-1
Acquiring a New IP Address and New Configuration Parameters 3-2
Acquiring the Same IP Address Again 3-5
Implementation Notes 3-6
Enabling DHCP Services 3-6
Enabling DHCP on an Interface 3-6
Accessing and Editing DHCP Parameters 3-7
Specifying Interfaces That Receive and Relay DHCP Packets 3-7
Specifying Servers for DHCP Services 3-8
Deleting DHCP from an IP Interface 3-8
Deleting DHCP Globally 3-8

Chapter 4
Configuring RARP Services

RARP Overview 4-1
Enabling RARP Services 4-2
Enabling RARP on an Interface 4-3
Accessing RARP Parameters 4-3
Disabling and Re-Enabling RARP Interfaces 4-4
Defining the RARP Mapping Table 4-5
Disabling RARP Globally 4-7
Deleting RARP Globally 4-8

Appendix A
Default Parameter Settings

SNMP Parameters A-1
BOOTP and DHCP Parameters A-3
RARP Parameters A-4

Index

Figures

Figure 1-1. Select Protocols Window 1-17
Figure 1-2. IP Configuration Window 1-18
Figure 1-3. Configuration Manager Window 1-21
Figure 1-4. Edit SNMP Global Parameters Window 1-21
Figure 1-5. SNMP Community List Window 1-24
Figure 1-6. SNMP Community Window 1-25
Figure 1-7. Delete SNMP Community Window 1-27
Figure 1-8. SNMP Manager List Window 1-28
Figure 1-9. Add SNMP Manager Window 1-28
Figure 1-10. SNMP Manager Window 1-29
Figure 1-11. Edit Thresholds Global Parameters Window 1-32
Figure 1-12. Thresholds Interface Lists Window 1-33
Figure 1-13. Threshold Configuration Window 1-34
Figure 1-14. Trap Configuration Window 1-40
Figure 1-15. Traps Exceptions Lists Window 1-42
Figure 1-16. Add Trap Window 1-42
Figure 2-1. Client and Server on the Same Physical Network 2-2
Figure 2-2. Client and Server on Different Physical Networks 2-2
Figure 2-3. BOOTREQUEST and BOOTREPLY Fields 2-3
Figure 2-4. BOOTP Relay Agent Interface Table Window 2-9
Figure 2-5. BOOTP Relay Agent Forwarding Table Window 2-12
Figure 2-6. BOOTP Addresses Window 2-12
Figure 2-7. BOOTP Client Interface Table Window 2-16
Figure 2-8. BOOTP Client Interface Address Window 2-16
Figure 2-9. BOOTP Relay Agent Preferred Server Table Window 2-18
Figure 2-10. BOOTP Preferred Server Configuration Window 2-19
Figure 3-1. Identifying DHCP Servers 3-2
Figure 3-2. Fields in a DHCP Packet 3-3

Figure 3-3. Requesting and Receiving IP Information 3-4
Figure 4-1. RARP Server Supplying an IP Address 4-1
Figure 4-2. RARP Interface Table Window 4-5
Figure 4-3. RARP Map Table Window 4-6
Figure 4-4. RARP Addresses Window 4-6
Figure 4-5. Edit RARP Global Parameters Window 4-8
Figure 4-6. Confirmation Window for Deleting RARP 4-8

Tables

Table 1-1. Severity Levels for Event Messages 1-7
Table 1-2. Example of Threshold and Severity Settings 1-7
Table 1-3. DRAM and RMON Memory Size 1-11
Table 1-4. Maximum Number of Hosts 1-13
Table 1-5. Default Size for Capture Buffer 1-15
Table A-1. SNMP Global Parameters A-1
Table A-2. SNMP Community Parameters A-1
Table A-3. SNMP Manager Parameters A-1
Table A-4. SNMP Threshold Global Parameters A-2
Table A-5. SNMP Threshold Interface Parameters A-2
Table A-6. SNMP Trap Interface Parameters A-2
Table A-7. BOOTP Relay Agent Interface Parameters A-3
Table A-8. BOOTP Addresses Parameters A-3
Table A-9. BOOTP Client Interface Address Parameters A-3
Table A-10. BOOTP Preferred Server Configuration Parameters A-4
Table A-11. RARP Interface Parameters A-4
Table A-12. RARP Address Parameters A-4

About This Guide

Read this guide to learn how to configure router or BNX software for the following services:

- Simple Network Management Protocol or SNMP (Chapter 1)
- Bootstrap Protocol or BOOTP (Chapter 2)
- Dynamic Host Configuration Protocol or DHCP (Chapter 3)
- Reverse Address Resolution Protocol or RARP (Chapter 4)

These services all use the Internet Protocol (IP) for message transport. To use one of these services on a router interface, you must enable IP services on that interface.

This guide provides the following information for each service:

- An overview of the protocol
- Issues you should consider when implementing the protocol
- Procedures for enabling the service on a Bay Networks router
- Procedures for tailoring parameters to meet your specific requirements

Software Suites

Routing and Switching software is available in the following suites:

- The *System Suite* includes IP routing, 802.1 Transparent Bridge, Source Route Bridge, Translation Bridge, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, and basic DLSw.
- The *LAN Suite* includes DECnet Phase 4, AppleTalk Phase 2, OSI, VINES, IPX, and ATM DXI, in addition to the System Suite.

- The *WAN Suite* includes ATM DXI, Frame Relay, LAPB, and X.25, in addition to the System Suite.
- The *Corporate Suite* includes the System, LAN, and WAN suites in their entirety.
- The *ARE ATM Suite* provides RFC 1483 and 1577 compliance, ATM UNI 3.0 signaling, in addition to the LAN Suite.
- The *ARE VNR Corporate Suite* provides ATM Forum LAN Emulation, in addition to the ARE ATM Suite and Corporate Suite.
- The *BNX Suite* includes IP Routing, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, File-Based Performance Statistics, Frame Relay switching, and Frame Relay billing, and selected components from the Corporate, ARE ATM, and ARE VNR Corporate suites.

Availability of features and functionality described in this guide depends on the suites you are using.

Audience

This guide addresses system and network managers who have some experience using Site Manager software to configure Bay Networks routers. If you have never used Site Manager software to configure Bay Networks routers, read *Using Site Manager Software* and *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, before you use this guide.

Bay Networks Customer Support

Bay Networks provides live telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers holding Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.
- In Germany, call 0130-37-32.
- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.
- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command GO BAYNETWORKS at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Conventions

This section describes the conventions used in this guide.

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**

arrow character (→)	Separates menu and option names in instructions. Example: Protocols→AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone:	1-800-845-9523
FAX - U.S./Canada:	1-800-582-8000
FAX - International:	1-916-939-1010

Acronyms

ASN.1	Abstract Syntax Notation One
BOOTP	Bootstrap Protocol
CMIP	Common Management Information Protocol
DCM	data collection module
DHCP	Dynamic Host Configuration Protocol
FDDI	Fiber Distributed Data Interface
IP	Internet Protocol
MAC	Media Access Control
PDU	protocol data unit
PVCs	permanent virtual circuits
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
RMON	remote monitoring
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol

Chapter 1
Configuring SNMP Services

You can tailor router or BNX software to take advantage of a variety of Simple Network Management Protocol (SNMP) services. Refer to this chapter for the following information:

- An overview of SNMP (see page 1-1)
- Additional resources that describe SNMP (see page 1-5)
- Features of the Bay Networks implementation of SNMP (see page 1-6)
- Instructions for enabling SNMP services (see page 1-16)
- Instructions for accessing and editing SNMP parameters (see page 1-20)

SNMP Overview

SNMP is a simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP *applications* (also called *SNMP managers*) and SNMP *agents*.

SNMP applications run in a network management station and issue queries to gather information about the status, configuration, and performance of external network devices (called *network elements* in SNMP terminology). The Bay Networks Site Manager software is an example of a network management station, and the Bay Networks backbone node (BN®) router is an example of a network element.

SNMP agents run in network elements (for example, in the BN) and respond to network management station queries (for example, from Site Manager). In addition, agents send unsolicited reports (called *traps*) back to the network management station when certain network activity occurs.

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request, by verifying that the manager belongs to an SNMP *community* with access privileges to the agent.

An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers. The community has a name, and all members of a community have the same access privileges: either read-only (members can view configuration and performance information) or read-write (members can view configuration and performance information, and also change the configuration).

All SNMP message exchanges consist of a community name and a data field, which contains the SNMP operation and its associated operands. You can configure the SNMP agent to receive requests and send responses only from managers that are members of a known community. If the agent knows the community name in the SNMP message and knows that the manager generating the request is a member of that community, it considers the message to be authentic and gives it the access allowed for members of that community. Thus, the SNMP community prevents unauthorized managers from viewing or changing the configuration of a router.

Remote Network Monitoring (RMON)

You can configure a data collection module (DCM) in the Bay Networks 8-port ANH™ to act as a remote monitoring (RMON) device, in compliance with RFC 1757. This RFC is an extension of SNMP, and specifies a standard MIB that defines both parameters for recording statistics and the actual statistics themselves. The purposes of RMON include

- Monitoring network performance

  You can configure the DCM to continuously perform diagnostics and monitor network performance. If a network failure occurs, the DCM can store statistical information about the failure. The management stations can use this information to investigate the cause of the failure.

- Detecting and reporting problems

  You can configure the DCM to recognize and continuously check for error conditions.

- Collecting information for problem solving

  You can configure the DCM to give management stations information they need to solve problems. For instance, the DCM can identify the hosts on a network that generate the most traffic or errors.

Refer to "SNMP Implementation Notes," later in this chapter, for issues you should consider when using a DCM for RMON.

The RMON Groups

The RMON agent runs on the DCM in the 8-port ANH, and comprises a set of MIB groups. RFC 1757 defines the function and organization of these groups. Bay Networks implements the following groups in its RMON agent for the 8-port ANH:

- Ethernet Statistics
- History Control
- Ethernet History
- Host
- HostTopN
- Matrix
- Filter
- Packet Capture

RMON groups contain *control* and *data tables*. Control tables contain *control parameters* that specify which statistics you want to access. You can view and change many entries in a control table. Data tables contain statistics the agent obtains, and usually you can only view entries in these tables.

Some of the groups work together to provide a particular RMON function. For example, the History Control group and Ethernet History group together provide the history capability in the RMON agent for the DCM.

The following sections indicate the function of each group and the tables that each group defines. Refer to RFC 1757 for the following information:

- A list of all the parameters that appear in a control table
- The read/write status of a control parameter
- The default values for control parameters with read/write status
- A list of all the objects that appear in a data table

Ethernet Statistics Group

The Ethernet Statistics group records data that the DCM measures on network interfaces. The DCM creates one entry for each Ethernet interface it monitors on a device and places the entry in the EtherStatsTable. The EtherStatsTable also contains control parameters for this group.

History Control Group

The History Control group manages the periodic statistical sampling of data from networks. This group specifies control parameters, such as the frequency of data sampling, in the historyControlTable.

Ethernet History Group

The Ethernet History group records periodic statistical samples from Ethernet networks, for example, interface addresses and polling periods. This group places the statistical samples in the etherHistoryTable.

Host Group

The Host group identifies hosts on the network by recording the source and destination MAC addresses in good packets, and places the information in the hostTable. This group also records the time it discovered a host on the network in the hostTimeTable. The hostControlTable specifies control parameters such as which monitoring operations the DCM performs, and contains some information about the monitoring process.

HostTopN Group

The HostTopN group ranks hosts according to a statistic type. For example, you might want to rank the hosts by the number of errors they generate. Control parameters for this group appear in the hostTopNControlTable, and data this group generates appears in the hostTopNTable. To use the HostTopN group, you must set up the Host group.

Matrix Group

The Matrix group stores statistics for an interchange between interfaces at different addresses. This group's control parameters, such as the interface that starts the interchange, appear in the matrixControlTable. When the Matrix group receives information from a good packet, it places data in both the matrixSDTable and the matrixDSTable.

Filter Group

The Filter group specifies what type of packets the DCM should capture. Filter control parameters, such as the minimum length of the packets to capture, appear in the filterTable. Associated with each filter is a *channel* (a specific path along which data flows). Control parameters in the channelTable define how and where the filtered packets flow.

Packet Capture Group

The Packet Capture group enables the capture of packets that satisfy the Filter group control parameters. Control parameters in the bufferControlTable specify how to transfer data from the channelTable to the captureBufferTable. For example, you can specify the maximum number of octets from each packet that the group should store in the captureBufferTable. To use the Packet Capture group, you must set up the Filter group.

For More Information about SNMP

The following documents provide more detail about SNMP design and implementation:

Rose, Marshall T. *The Simple Book.* Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1991.

Stallings, William. *SNMP, SNMP v2, and CMIP: The Practical Guide to Network-Management Standards.* Reading, Massachusetts.: Addison-Wesley Publishing Co., Inc., 1993.

SNMP Implementation Notes

This section contains information about features specific to the Bay Networks implementation of SNMP.

Internet Protocol (IP)

SNMP uses the User Datagram Protocol (UDP) to transport its messages. You must enable IP in order to use UDP and SNMP.

Thresholds

SNMP uses a MIB (Management Information Base) to manage the router. The MIB includes an extensive collection of statistics (MIB *variables*) that track the router's performance and provide early warnings of abnormal operating conditions.

With the Site Manager threshold feature, you can configure the agent to automatically notify the network manager when specific statistics (or *instances* of the variable) reach certain levels.

You can set a threshold for any integer, counter, gauge, or time-tick variable in the MIB. Using the threshold parameters (refer to "Editing Threshold Parameters" later in this chapter), you select the polling interval, which specifies how often the agent checks the statistic to see if its value has reached the threshold. You also set three threshold values (high, medium, and low) and specify the threshold action as *Lessthan* or *Greaterthan* (refer to "Threshold Example," later in this chapter).

When the statistic reaches the threshold, the agent generates an event. You specify the severity level at which you want the manager to log the event. Table 1-1 lists the available severity levels and their suggested meanings. Depending on how you configure the SNMP trap parameters (refer to "Configuring Traps" later in this chapter), the agent may also send the threshold exception as an SNMP trap.

Table 1-1. Severity Levels for Event Messages

Severity	Suggested Definition
Info	Indicates routine events that require no action
Warning	Indicates events that occur unexpectedly
Debug	Indicates events that you use to solve network problems

Threshold Example

Suppose (while running BNX software) you want SNMP to warn you if the number of high-priority (Priority Level 1) packets queued for transmission is approaching the maximum number supported by an interface. This maximum value is specified by the wfCctOptsCngcCfgQp1Threshold MIB object. Using the threshold parameters, you set a threshold for wfCctOptsCngcCfgQp1Threshold. For the sake of the following example, assume that wfCctOptsCngcCfgQp1Threshold is equal to 255 (the maximum value for a synchronous circuit).

You also set the polling interval to twenty seconds, to indicate that, every twenty seconds, the agent should check variables for which you have configured thresholds. You set the threshold action to *Greaterthan* and set the threshold levels and severity of events to the values listed in Table 1-2.

Table 1-2. Example of Threshold and Severity Settings

Threshold Level	Low	Medium	High
Depth of Priority 1 transmit queue	102 (40% of capacity)	153 (60% of capacity)	205 (80% of capacity)
Severity of event	INFO	INFO	WARNING

When you add this threshold to the MIB, the agent polls the variable wfCctOptsCngcCfgQp1Threshold every twenty seconds and responds as follows:

- If its value is greater than 102, but less than or equal to 153, the manager logs an informational event indicating that the queue depth exceeded the low threshold.

- If its value is greater than 153 but less than or equal to 205, the manager logs an informational event indicating that the queue depth exceeded the medium threshold.
- If its value is greater than 205, the manager logs a warning event indicating that the queue depth exceeded the high threshold.

Event Message Format

By default, the threshold event messages include the OID (MIB object identifier) of the variable that exceeded the threshold, the value of the variable, and the threshold level exceeded.

For example, if the wfCctOptsCngcCfgQp1Threshold variable has a value of 120, the agent generates an event message similar to

```
#1:08/27/93 10:53:20.802 INFO SLOT 2 STA CODE: 6
Object 1.3.6.1.4.1.18.3.5.1.4.10.1.24 with value = 120 units/ hour is >
low threshold.
```

You can, however, identify objects more easily by configuring the software to report the object name rather than the OID in the event message. To configure the software to report the object name in the event message, use the Threshold Label parameter (refer to “Editing Threshold Parameters” later in this chapter).

For example, if you set the Threshold Label parameter to **wfCctOptsCngcCfgQp1Threshold**, the agent generates an event message similar to the following one:

```
#1:08/27/93 10:53:20.802 INFO SLOT 2 STA CODE: 6
Object wfCctOptsCngcCfgQp1Threshold with value = 120 units/ hour is > low
threshold.
```

State of a Threshold

If the collision rate stays above a threshold for an extended period of time, the agent continues to generate a new event every five seconds. You can specify the maximum number of event messages you want the agent to generate before it changes the threshold’s state to *held*.

When the threshold is in a held state, the agent does not generate new events unless the statistic exceeds the threshold at a different level. If the statistic does not exceed any threshold for a specified number of polling periods, the agent no longer considers the threshold held.

Memory Considerations

Polling statistics to determine whether they have reached a threshold and reporting events when variables exceed thresholds requires router processing capacity. When you set more thresholds and use shorter polling intervals, the performance of the router will probably decline.

Traps

Using the SNMP trap parameters, you can configure which event log messages the agent sends to the network management station as traps. You select the traps the agent sends based on slot, protocol entity, and severity level. You can also specify up to 50 *exceptions*, traps that the agent always sends, or never sends, regardless of slot and regardless of how you configure the trap parameters. Refer to "Editing Trap Parameters" later in this chapter for information on how to specify which traps the agent sends.

RMON

When you enable a DCM, you automatically set up RMON Statistics and History configurations; you can also choose to set up Matrix and Host configurations. Use Site Manager to enable a DCM (refer to *Connecting AN and ANH Systems to a Network* for details). To set up other RMON configurations and to view RMON statistics, use Optivity® LAN or a third-party RMON network management application.

You can use the Technician Interface to modify DCM or RMON parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software.*

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

In addition, be sure to avoid running scripts that continually issue Technician Interface commands while you are running another RMON network management application. This combination can cause the SNMP agent to fill the system buffers with RMON data, leading to a system restart.

Read the following sections to learn about RMON memory use and interoperability issues you should consider when using RMON network management applications with the DCM. These sections assume that you have a good understanding of each RMON group, and do not refer to the low-level details of the MIB, such as RMON MIB objects. Refer to "Remote Network Monitoring (RMON)," earlier in this chapter, and RFC 1757 for information about each RMON group.

RMON Interoperability Issues

Some network management applications automatically set up their own configurations for an RMON group, without checking to see if the RMON agent already has a default configuration. In addition, when you terminate those applications, they may not remove the configurations they set up for the RMON agent. These features can result in the RMON agent using excessive amounts of memory and processing power.

Example

When you enable a DCM, the RMON agent automatically creates a History configuration. Suppose you then start a third-party RMON History application, which creates its own History configuration for the agent. The RMON agent stores the data in two places, wasting memory.

In addition, when you terminate the third-party RMON application, it does not remove its History configuration, using memory and processing power indefinitely.

You can only release these resources by using another application, such as the SNMP tool or network management station, or by resetting the DCM. If you use too many resources for an RMON task, the DCM can run out of memory for other RMON tasks and performs more slowly.

RMON Memory Use

The total amount of RMON memory depends on the DRAM in the DCM (Table 1-3).

Table 1-3. DRAM and RMON Memory Size

Installed DRAM (MB)	RMON Memory in Bytes
2	162,578
4	2,077,330
8	5,222,034
16	12,561,042

Note: *If the RMON memory pool is full or if the RMON agent reaches an implementation limit, the agent responds to an SNMP* SET *command on an RMON control table entry with an SNMP GEN-ERROR.*

The following sections describes how much memory you need to

- Configure an RMON group (for example, to configure the Matrix group or to configure Filter and Packet Capture groups).
- Store the data for an RMON group (for example, to store the packets a DCM captures).

In the following sections, the word *configuration* means the set of control tables for a group. For example, a Matrix configuration includes only the matrixControlTable. Note that you can create more than one configuration for some RMON groups. For example, you can create more than one History configuration, allowing you to specify different intervals for sampling statistics.

Interoperability Issues and Memory Use for RMON Groups

You should understand the following issues about each RMON group's memory requirements and ability to operate with third-party RMON network management applications.

Statistics Group

When you enable the DCM, the RMON agent automatically creates a Statistics configuration that records data for each network interface. Through your RMON network management application, you can create as many Statistics configurations as memory permits, up to the RMON limit of 65,535 configurations.

If you create multiple configurations, it is possible to collect the same set of statistics for the same interface in multiple data tables. The absolute values of those statistics may vary from table to table, since the baseline of each statistics counter occurs when you create a configuration. You may prefer, however, to use only one Statistics configuration, to conserve memory for other RMON groups.

You need 200 bytes of memory for each Statistics configuration.

History Group

When you enable the DCM, the RMON agent automatically creates a History configuration that collects History data at two intervals. The first configuration provides short-term history by sampling statistics every 30 seconds and holding up to 50 samples (in RMON terms, “buckets”). The second configuration provides long-term history by sampling statistics every 30 minutes and holding up to 50 buckets.

Through your RMON network management application, you can create as many History configurations as memory permits, up to the RMON limit of 65,535 configurations.You can also set the number of buckets a particular History configuration uses to as many as available memory allows. If you request more buckets than memory allows, the agent allocates enough buckets to fill available memory.

You need 504 bytes of memory for each History configuration (252 bytes each for the short-term and long-term History configurations).

The History data requires 52 bytes of memory per bucket. You calculate the total memory (in bytes) you need to store the data as follows:

Number of buckets * 52 * 2 History configurations

This calculation shows that you need approximately 5.1 KB for the default setting of 50 buckets.

Host Group

When you enable the DCM, the default setting (Enabled) for the RMON Default Host parameter creates a Host configuration. To prevent creation of a Host configuration, set the RMON Default Host parameter to Disable before you enable the DCM (refer to *Connecting AN and ANH Systems to a Network* for details).

Some RMON network management applications expect the DCM to set up a Host configuration, while others set up their own configurations.

Note: *The RMON agent allows you to create only one Host configuration. Be sure to set the RMON Default Host parameter according to the expectations of the RMON network management application.*

The Host configuration requires 148 bytes. The Host data requires 105 bytes of memory per host address the DCM detects on a segment.

You specify the maximum number of host addresses that appear in the Host configuration by setting the RMON Max Host parameter when you enable a DCM. If there is not enough memory for the number of hosts you request, the RMON agent sets the RMON Max Host parameter to the highest possible value. The number of addresses can range from 100 to 8,128 hosts, depending on the DCM memory configuration. Table 1-4 shows recommended values for this parameter.

Table 1-4. Maximum Number of Hosts

Installed DRAM (MB)	Maximum Number of Hosts
2–4	2,048
5–8	4,096
9–16	8,128

You calculate the total memory (in bytes) you need for the host data as follows:

105 * Value of the RMON Max Host parameter

HostTopN Group

To save memory and increase performance, there is no default configuration for the HostTopN group. You must create HostTopN configurations through your RMON network management application. You can create as many HostTopN configurations as memory permits, up to the RMON limit of 65,535 configurations.

Note: *Before you create a HostTopN configuration, you must create a Host configuration.*

Each HostTopN configuration requires 164 bytes. The HostTopN data requires 10 bytes of memory per host address the DCM detects on a segment.

You calculate the total memory (in bytes) you need for the HostTopN data as follows:

10 * Value for the RMON Max Host parameter

Refer to the previous section for information on setting the RMON Max Host parameter.

Matrix Group

When you enable the DCM, the default setting (Enabled) for the RMON Default Matrix parameter causes the DCM to set up a Matrix configuration. To prevent creation of a Matrix configuration, set the RMON Default Matrix parameter to Disable before you enable the DCM (refer to *Connecting AN and ANH Systems to a Network* for details).

Some RMON network management applications expect the DCM to set up a Matrix configuration, while others set up their own configurations.

Note: *The RMON agent allows you to create only one Matrix configuration. Be sure to set the RMON Default Matrix parameter according to the expectations of the RMON network management application.*

The Matrix configuration requires 212 bytes. The Matrix data requires approximately 178 bytes of memory per source/destination pair the DCM detects on a segment.

Filter and Capture Groups

Caution: *The memory you need for a Filter/Capture configuration and for storing captured packets can easily exhaust all the available memory on a DCM, particularly if the filters are not selective.*

You must create Filter and Capture configurations through your RMON network management application. You can create as many filters and capture buffers as memory permits, up to the RMON limit of 65,535 configurations.

Memory requirements vary greatly according to the size and number of the filters and the size of the capture buffer. In most cases, you need 3 to 5 KB of memory for the Filter and Packet Capture configuration.

The size of the capture buffer determines the amount of memory you need for the data. You can request the largest buffer size available by specifying a buffer size of -1 through your RMON network management application. When you specify -1 for the capture buffer size, the agent attempts to allocate a default buffer depending on the DRAM in the DCM (Table 1-5).

Table 1-5. Default Size for Capture Buffer

Installed DRAM (MB)	Default Size (KB)
2	32
4	64
8	256
16	512

You can also request a larger buffer size up to 15 MB. In any case, if there is not enough memory currently available to satisfy the request, the agent will provide a buffer that uses all available memory.

You can determine the maximum number of packets that an agent can capture in a buffer as follows:

buffer size/(packet slice size + 20 bytes)

Example

You specify a buffer size of 32 KB and a packet slice size of 1 KB. After checking the available memory, the RMON agent allocates the buffer size you requested. The buffer can hold a maximum of 32,768 / (1024 + 20) or 31 packets.

Note: *The RMON agent allocates the full amount of memory you specify for the packet slice size to each packet, even if the packet size is smaller than this amount. For this reason, Bay Networks recommends that you set the packet slice size to the smallest size possible. The maximum packet size is 2 KB.*

Enabling SNMP Services

You must enable IP services to use SNMP. When you enable IP services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

This section assumes that you have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, and that you have

1. Opened a configuration file
2. Specified router hardware if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling IP services, or configured a WAN circuit if this connector requires one

Enabling IP on an Interface

When you select a link or net module connector, or when you finish configuring a WAN circuit, the Select Protocols window appears (Figure 1-1).

Note: *The window varies slightly according to circuit type, displaying only those protocols that the circuit type supports.*

Figure 1-1. Select Protocols Window

To enable IP on an interface:

1. **Select IP from the Select Protocols menu.**
2. **Click on OK.**

   The IP Configuration window appears (Figure 1-2).

Figure 1-2. IP Configuration Window

3. **Edit the parameters in the window.**

   Use the descriptions that follow as a guide.

4. **Edit or accept the default values for the remaining IP interface parameters, as follows:**

   - **To accept the default values, click on OK.**

   Site Manager displays the Configuration Manager window. You can now customize SNMP parameters for the IP interface (refer to “Accessing SNMP Parameters”).

   - **To edit all IP interface parameters, click on Details.**

   Refer to *Configuring IP Services* for information about editing IP interface parameters.

Parameter:	**IP Address**
Default:	None
Options:	Any valid IP address
Function:	Assigns a 32-bit IP address to the interface.
Instructions:	Enter the IP address of the interface in dotted decimal notation. Enter 0.0.0.0 to configure an unnumbered interface on the circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.1.4

Parameter:	**Subnet Mask**
Default:	The Configuration Manager automatically calculates an appropriate subnet mask, depending on the class of the network to which the interface connects.
Options:	Any valid IP address
Function:	Specifies the network and subnetwork portion of the 32-bit IP address.
Instructions:	Accept the assigned subnet mask, or enter another subnet mask in dotted decimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.1.6

Parameter:	**Transmit Bcast Addr**
Default:	0.0.0.0
Options:	0.0.0.0 or any valid IP broadcast address
Function:	Specifies the address that this IP subnet uses for broadcasting packets. Accepting 0.0.0.0 for this parameter specifies that the IP router uses a broadcast address with a host portion of all 1s; it does not configure the router to use the address 0.0.0.0 to broadcast packets. For example, if you have IP address 123.1.1.1 and a subnet mask of 255.255.255.0, accepting the default value 0.0.0.0 configures the IP router to use the address 123.1.1.255 to broadcast packets.
Instructions:	Accept the default, 0.0.0.0, unless the calculated broadcast address (host portion) of all 1s is not adequate. If this is the case, then enter the appropriate IP broadcast address in dotted decimal notation. To set the explicit broadcast address of all 1s, enter 255.255.255.255.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.1.8

Parameter:	**UnNumbered Assoc Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies an address that IP uses when sourcing a packet.
	Routing Information Protocol (RIP) uses this address to make decisions about advertising subnets over the unnumbered interface if the subnets have the same mask as the associated address.
Instructions:	Specify the address of any numbered interface on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.1.110

Accessing SNMP Parameters

Use the Configuration Manager to edit SNMP parameters for IP interfaces.

Note: *The instructions in this section assume that you have already configured at least one IP interface. If you have not yet configured an IP interface, or want to add additional IP interfaces, refer to "Enabling SNMP Services" for instructions.*

You access all SNMP parameters from the Configuration Manager window (Figure 1-3). Refer to the book *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for instructions on accessing this window.

For each SNMP parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software.*

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

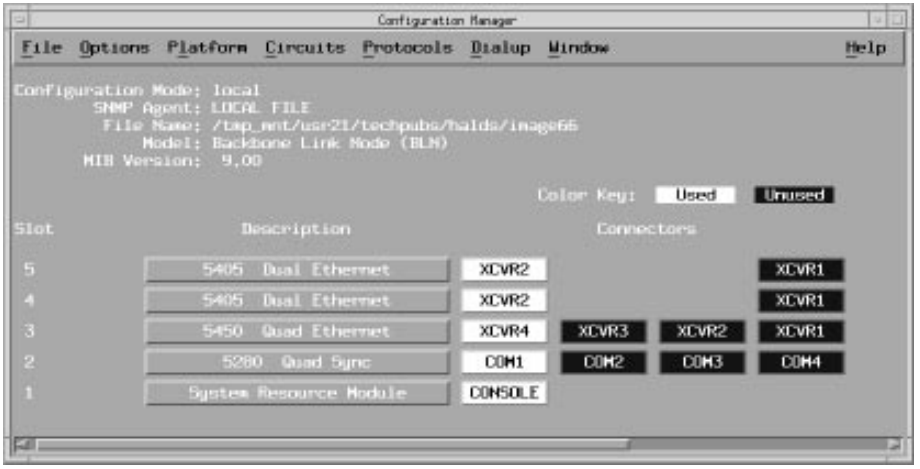


Figure 1-3. Configuration Manager Window

Editing SNMP Global Parameters

To edit SNMP global parameters, begin at the Configuration Manager window (Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Global.**

   The Edit SNMP Global Parameters window appears (Figure 1-4).

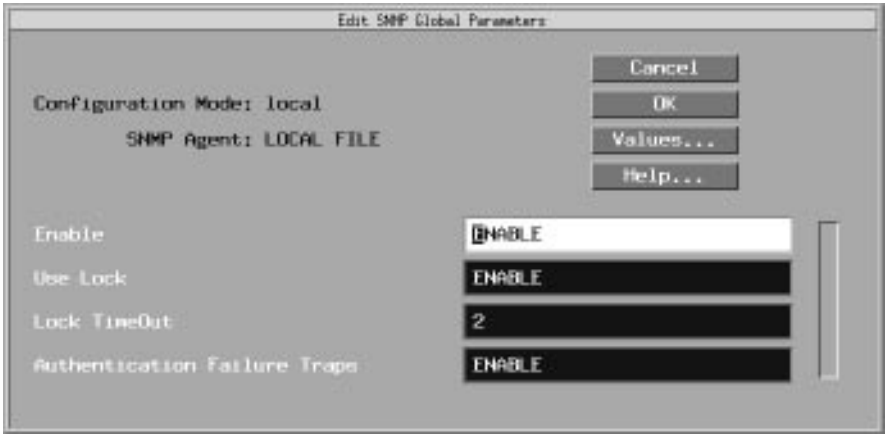


Figure 1-4. Edit SNMP Global Parameters Window

2. **Edit the parameters in this window.**

   Use the descriptions that follow as a guide.

3. **Click on OK.**

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state of the SNMP agent on all interfaces that support IP.
Instructions:	Select Enable to enable the SNMP agent. Select Disable to disable the SNMP agent.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.1

Caution: *When you disable the SNMP agent in dynamic mode, you immediately prohibit Site Manager from communicating with the router.*

Parameter:	**Use Lock**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the agent responds to multiple network management stations issuing simultaneous SNMP SET commands to the router. When you set this parameter to Enable, the agent identifies the station from which it receives the next SNMP SET command and, for a time equal to the value of the Lock TimeOut parameter, responds only to SNMP SET commands from that station. If the agent receives an SNMP SET command from another network management station during this time, it issues an SNMP genErr GetResponse PDU, which that station logs as an SNMP SET ERROR message.
Instructions:	Select Enable to prohibit the agent from responding to simultaneous SNMP SET commands from multiple network management stations. Select Disable to allow the agent to respond to simultaneous SNMP SET commands from multiple network management stations.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.2

Parameter:	**Lock TimeOut**
Default:	2 minutes
Range:	1 to 60 minutes
Function:	Specifies the maximum number of minutes the agent allows an idle network management station to hold a lock on it. During this time, the agent locks out SNMP SET command from other network management stations. The lock timer is reset each time the locking manager issues an SNMP SET command.
Instructions:	Enter the number of minutes only if you set Use Lock to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.4

Parameter:	**Authentication Failure Traps**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the router attempts to generate an Authentication Failure trap when it receives an SNMP message from an SNMP manager falsely claiming to be in a particular community or specifying an unknown community.
Instructions:	Select Enable to enable the router to generate Authentication Failure traps. If you select Enable, you must configure an SNMP manager to receive the trap. You configure a trap from the Trap Configuration window. Select Disable to prohibit the router from generating Authentication Failure traps.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.35

Editing SNMP Community Parameters

This section describes how to add, edit, and delete the SNMP communities to which the SNMP agent responds or sends traps. It also describes how to select which managers are members of a particular community.

Note: *When you add the first IP interface during a local configuration, Site Manager automatically creates a read-write public community with a wildcard manager (0.0.0.0). For security reasons, we recommend that you replace the public community and wildcard manager with a unique community specifying a limited list of managers.*

Adding an SNMP Community

To add an SNMP community, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (Figure 1-5).

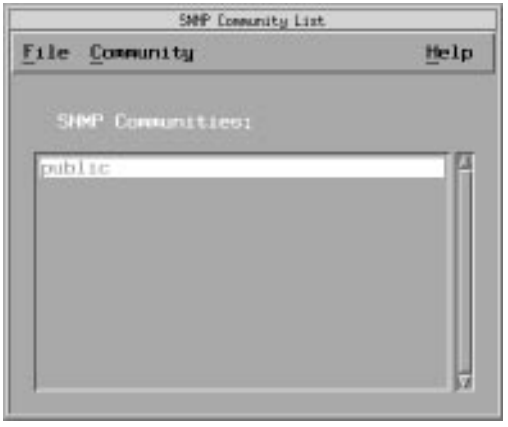


Figure 1-5. SNMP Community List Window

2. **Select Community→Add Community.**

   The SNMP Community window appears (Figure 1-6).

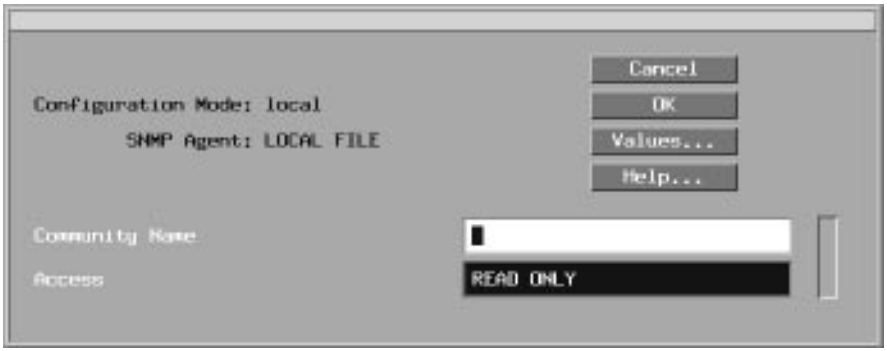


Figure 1-6. SNMP Community Window

3. **Edit the parameters.**

   Use the descriptions that follow as a guide.

4. **Click on OK.**

   The new SNMP community appears in the SNMP community list window.

5. **Specify the members of the community.**

   Refer to "Adding a Manager," later in this chapter, for instructions.

Parameter:	**Community Name**
Default:	None
Options:	Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces
Function:	Specifies the name of the SNMP community.
Instructions:	Enter the SNMP community name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.2.1.3

Parameter:	**Access**
Default:	Read Only
Options:	Read Only | Read-Write
Function:	Specifies the access privileges that the router grants to all members of this SNMP community.
Instructions:	Select Read Only to allow all members of this community to only view configuration and performance information about this router. Select Read-Write to allow all members of this community to both view configuration and performance information about this router and to change the router's configuration.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.2.1.4

Editing an SNMP Community

To edit an SNMP community, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (refer to Figure 1-5).

2. **Select the community you want to edit.**

3. **Select Community→Edit Community.**

   The SNMP Community window appears (refer to Figure 1-6).

   You can change both the name and the access privilege for the community. Refer to the previous section, "Adding an SNMP Community," for instructions on how to configure these parameters.

   If you want to add, edit, or delete community members from this community, refer to the section "Configuring SNMP Community Members," later in this chapter.

Deleting an SNMP Community

To delete an SNMP community, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (refer to Figure 1-5).

2. **Select the community you want to delete.**
3. **Select Community→Delete Community.**

   The Delete SNMP Community window appears (Figure 1-7).

Figure 1-7. Delete SNMP Community Window

4. **Make sure the correct SNMP community name appears in the window.**

   Click on Cancel if you do not want to delete the selected community.
5. **Click on Delete.**

Configuring SNMP Community Members

You can add, edit, and delete SNMP community members (called *managers*).

Adding a Manager

To add a manager, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (refer to Figure 1-5).
2. **Select the community to which you want to add managers.**
3. **Select Community→Managers.**

   The SNMP Manager List window for that community appears (Figure 1-8).

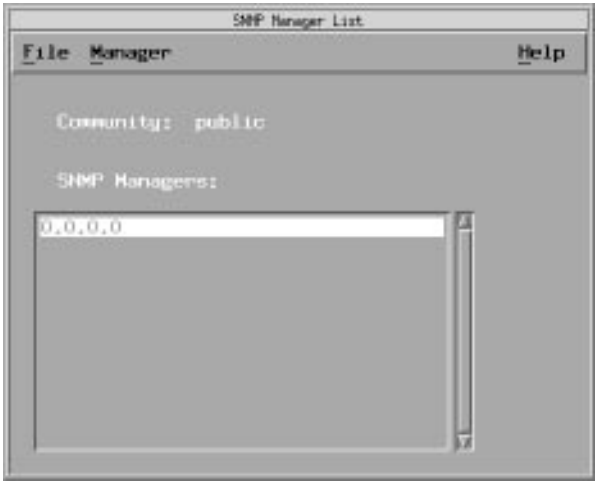


Figure 1-8. SNMP Manager List Window

4. **Select Manager→Add Manager.**

   The Add SNMP Manager window appears (Figure 1-9).

Figure 1-9. Add SNMP Manager Window

5. **Type in the IP address of the SNMP manager you want to add.**
6. **Click on OK.**
7. **Configure the manager to receive traps from the agent.**

   Refer to the following section for instructions.

Editing a Manager

When you edit a manager, you determine whether the manager receives traps and what types of traps the agent transmits to that manager. To edit a manager, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (refer to Figure 1-5).

2. **Select the community for which you want to edit the manager.**

3. **Select Community→Managers.**

   The SNMP Manager List window for that community appears (refer to Figure 1-8).

4. **Select the manager you want to edit.**

5. **Select Manager→Edit Manager.**

   The SNMP Manager window appears (Figure 1-10).

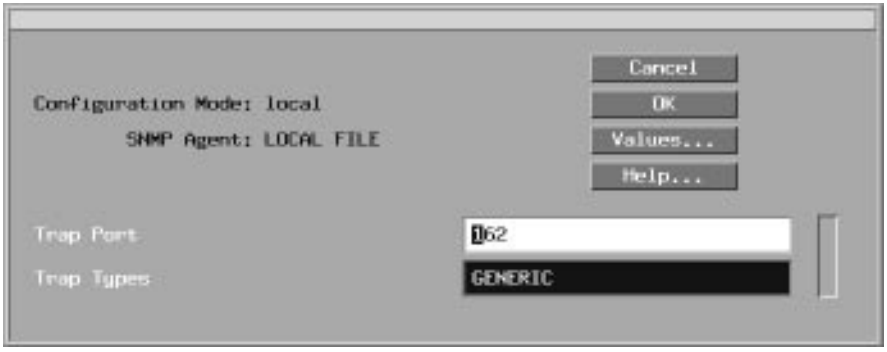


Figure 1-10. SNMP Manager Window

6. **Edit the parameters in this window.**

   Use the descriptions that follow as a guide.

7. **Click on OK.**

Parameter:	**Trap Port**
Default:	162
Range:	1 to 9999
Function:	Specifies the number of the port on the managing station to which the agent transmits traps.
Instructions:	The standard port number for trap messages is 162; however, you may enter a different port number. Be sure that you do not specify a port that another application uses.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.3.1.5

Parameter:	**Trap Types**
Default:	Generic
Options:	None | Generic | Specific | All
Function:	Specifies the type of trap the agent transmits to this manager.
Instructions:	Select None to prohibit the agent from transmitting traps to this manager. Select Generic to configure the agent to transmit the well-defined SNMP traps (cold-start, warm-start, and Authentication Failure traps) to the manager. The well-defined cold-start and warm-start traps are automatically active in the SNMP agent; however, you must enable the Authentication Failure Traps parameter for the agent to transmit such traps to this manager. Select Specific to configure the agent software to transmit all enabled log event traps to this manager. Select All to transmit cold-start traps, warm-start traps, and all enabled log event traps to this manager.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.3.1.6

Deleting a Manager

To delete a manager from an SNMP community, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (refer to Figure 1-5).

2. **Select the community from which you want to delete the manager.**

3. **Select Community→Managers.**

   The SNMP Manager List window for that community appears (refer to Figure 1-8).

4. **Select the manager you want to delete.**

5. **Select Manager→Delete Manager.**

   The Delete SNMP Manager window appears.

6. **Make sure the correct manager IP address appears.**

7. **Click on Delete.**

Editing Threshold Parameters

You can configure thresholds for any integer, counter, gauge, or time-tick variable in the MIB. Refer to the section “SNMP Implementation Notes” earlier in this chapter for more information about using thresholds.

This section describes all individual threshold parameters, and how to configure the threshold polling interval.

Configuring the Threshold Polling Interval

To set the polling interval, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→Global Protocols→Thresholds→Global.**

   The Edit Thresholds Global Parameters window appears (Figure 1-11).

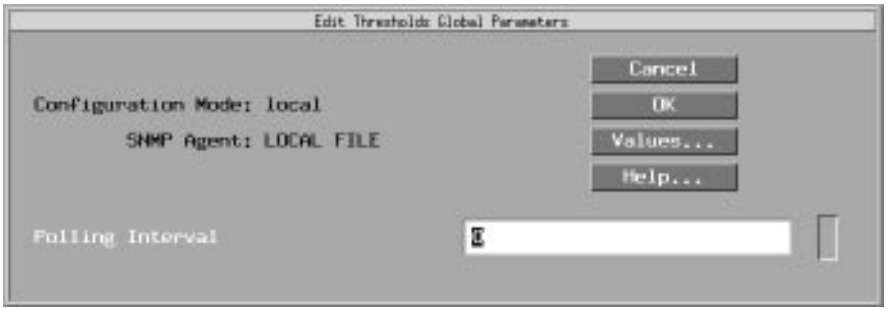


Figure 1-11. Edit Thresholds Global Parameters Window

2. **Specify the polling interval.**

   Use the description that follows as a guide.

3. **Click on OK to exit the window.**

Parameter:	**Polling Interval**
Default:	60 seconds
Range:	5 seconds minimum; no maximum value
Function:	Sets the time interval at which the agent polls the variable to determine whether that variable has reached the threshold.
Instructions:	Specify the number of seconds for the polling interval. Remember that the more often the agent polls the variable, the more memory it needs to manage the thresholds for this statistic.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.1.2

Configuring a Threshold

To configure a threshold you must have a good understanding of the MIB and be able to identify the instances of MIB objects to which you want to apply a threshold. For complete information about identifying a MIB object or an instance identifier, refer to the statistics section of *Managing Routers and BNX Platforms*.

To set a threshold, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→Global Protocols→Thresholds→Thresholds.**

   The Thresholds Interface Lists window appears (Figure 1-12).

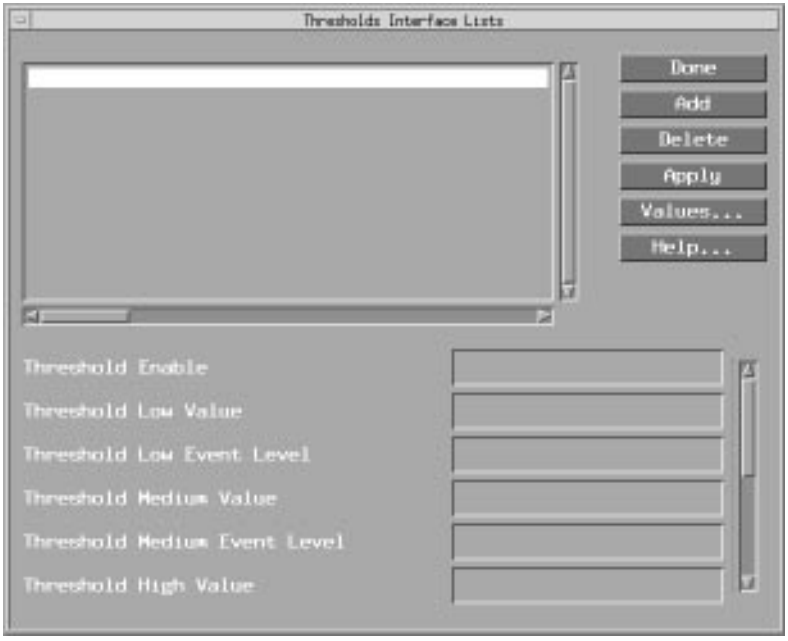


Figure 1-12. Thresholds Interface Lists Window

2. **Click on Add.**

   The Threshold Configuration window appears (Figure 1-13), displaying a list of all MIB objects the agent supports.

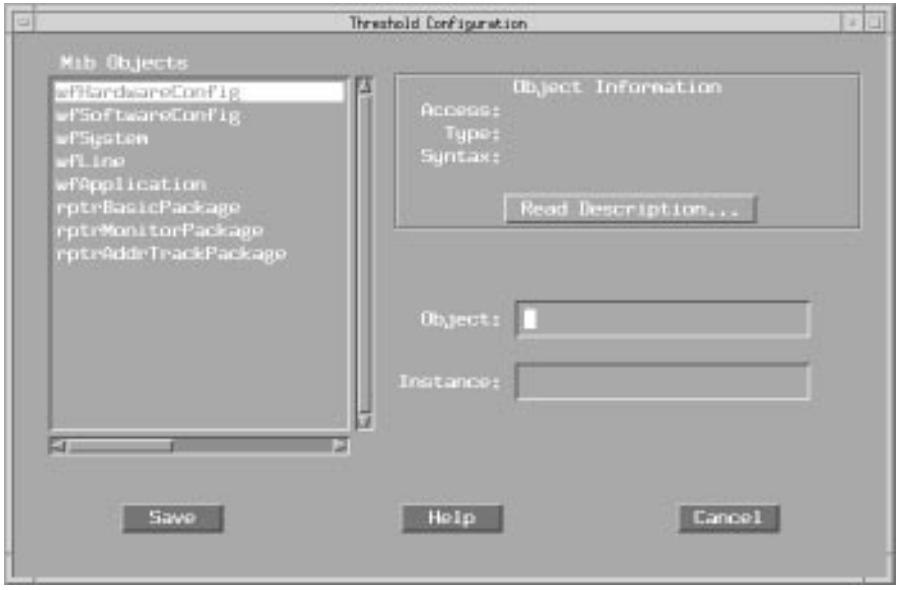


Figure 1-13. Threshold Configuration Window

3. **Select the object to which you want to apply a threshold.**

   The object appears in the Object field.

4. **Enter the instance identifier in the Instance field.**

5. **Click on Save.**

   The Threshold Interface Lists window appears again.

6. **Edit the Threshold Interface parameters.**

   Use the descriptions that follow as a guide.

7. **Click on Apply.**

8. **Repeat Steps 2 through 7 for other thresholds you want to add.**

9. **Click on Done when you have finished adding thresholds.**

Parameter:	**Threshold Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Toggles on and off the threshold for this variable.
Instructions:	Select Enable if you want the agent to apply the threshold to this variable. Select Disable if you want the agent to ignore the threshold for this variable.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.2

Parameter:	**Threshold Low Value**
Default:	0
Options:	Any integer value
Function:	Sets the value of the low threshold for this variable.
Instructions:	Specify the level at which you want the agent to generate a low-threshold exception event.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.5

Parameter:	**Threshold Low Event Level**
Default:	Info
Options:	Info | Warning | Debug
Function:	Specifies the severity level of the event message the agent generates when a variable exceeds the low threshold.
Instructions:	Select Info if you want low-threshold exceptions to generate routine events that require no action. Select Warning if you want low-threshold exceptions to generate events that indicate an unexpected situation occurred. Select Debug if you want low-threshold exceptions to generate events you use to solve network problems.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.6

Parameter:	**Threshold Medium Value**
Default:	0
Options:	Any integer value
Function:	Sets the value of the medium threshold for this variable.
Instructions:	Specify the level at which you want the agent to generate a medium-threshold exception event.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.7

Parameter:	**Threshold Medium Event Level**
Default:	Info
Options:	Info | Warning | Debug
Function:	Specifies the severity level of the event message the agent generates when a variable exceeds the medium threshold.
Instructions:	Select Info if you want medium-threshold exceptions to generate routine events that require no action. Select Warning if you want medium-threshold exceptions to generate events that indicate an unexpected situation occurred. Select Debug if you want medium-threshold exceptions to generate events you use to solve network problems.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.8

Parameter:	**Threshold High Value**
Default:	0
Options:	Any integer value
Function:	Sets the value of the high threshold for this variable.
Instructions:	Specify the level at which you want the agent to generate a high-threshold exception event.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.9

Parameter:	**Threshold High Event Level**
Default:	Info
Options:	Info | Warning | Debug
Function:	Specifies the severity level of the event message the agent generates when a variable exceeds the high threshold.
Instructions:	Select Info if you want high-threshold exceptions to generate routine events that require no action. Select Warning if you want high-threshold exceptions to generate events that indicate an unexpected situation occurred. Select Debug if you want high-threshold exceptions to generate events you use to solve network problems.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.10

Parameter:	**Threshold Units**
Default:	Persecond
Options:	Persecond | Absolute
Function:	Specifies the units used to determine whether a variable has exceeded a threshold.
Instructions:	Select Persecond if you want the agent to generate a threshold event when the variable's rate of change *per second* reaches one of the three thresholds. Select Absolute if you want the agent to generate a threshold event when the value of the variable reaches one of the three thresholds.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.12

Parameter:	**Threshold Action**
Default:	Greaterthan
Options:	Greaterthan | Lessthan
Function:	Specifies when the agent generates a threshold event.
Instructions:	Select Greaterthan if you want to record threshold events when the value of the variable is *greater than* the threshold specified. Select Lessthan if you want to record threshold events when the value of the variable is *less than* the threshold specified.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.13

Parameter:	**Threshold Max Successive Alarms**
Default:	5
Options:	Any integer value
Function:	Specifies the maximum number of successive alarms that the agent generates for this variable. A successive alarm represents two or more polling periods when the agent generates an alarm as a result of an exception at the same threshold level.
Instructions:	Specify the maximum number of successive alarms. When the agent exceeds the maximum number of alarms, it marks the threshold as held. The agent generates no more alarms until the variable either crosses the threshold at a different level or crosses no threshold for the number of polling intervals equal to the value of the Threshold HoldDown Intervals parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.14

Parameter:	**Threshold HoldDown Intervals**
Default:	1
Options:	Any integer value
Function:	Specifies the number of exception-free polling intervals through which a variable in a held state must pass before the variable is no longer considered held.
Instructions:	Specify the number of exception-free polling intervals. The lower the number you select, the more likely the agent is to generate repetitive event messages for a variable that is intermittently exceeding thresholds.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.15

Parameter:	**Threshold Label**
Default:	ASN.1 object identifier
Options:	ASN.1 OID | String identifier
Function:	This parameter lets you enter a name for the object in string format to replace the ASN.1 object identifier. The string you enter appears in the log file, making it easier to identify the object that is the subject of the trap.
Instructions:	Type a name for the object, or leave this field empty to use the ASN.1 object identifier.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.22

Editing Trap Parameters

You can specify which traps the SNMP agent sends to the network management station.

Configuring Traps

To specify which traps the agent sends, based on slot, protocol entity, and severity level, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Trap Configuration→Interfaces.**

   The Trap Configuration window appears (Figure 1-14).

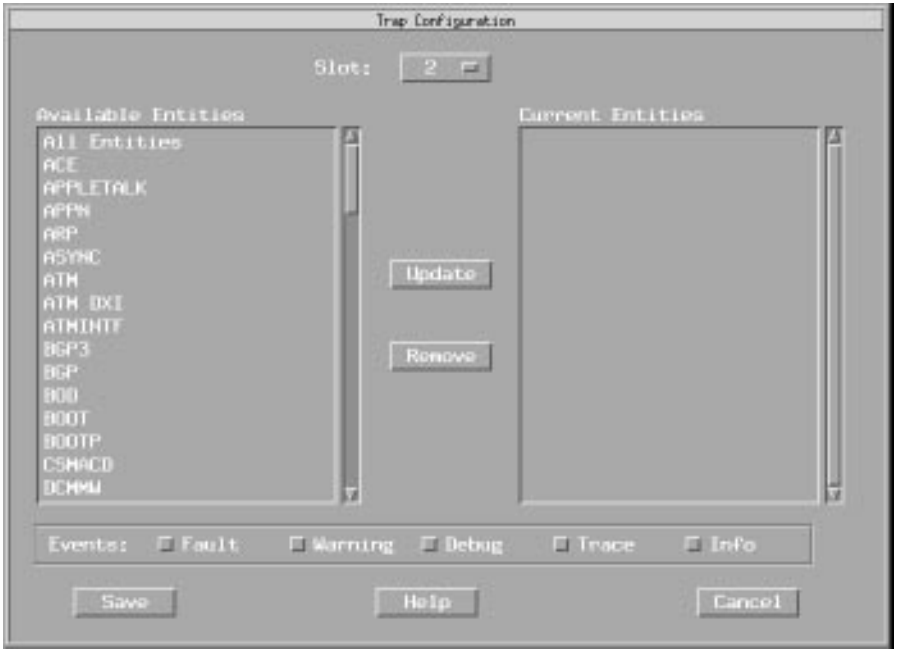


Figure 1-14. Trap Configuration Window

2. **Select the slot for which you want to configure traps.**

   You select a slot by clicking on the bar in the Slot box.

3. **Select an entity for which you want to configure traps.**

   The protocol entity names appear in the Available Entities column, a comprehensive list of all protocols available, regardless of the platform or software you are using.

   If you want to configure traps for all entities running on this slot, select All Entities from the top of the column.

4. **Select the severity levels for which you want to receive traps.**

   You select a severity level by clicking on the Events boxes at the bottom of the window. Refer to *Event Messages for Routers and BNX Platforms* for a definition of the severity levels.

5. **Click on Update.**

   The entity name moves to the Current Entities column, indicating that you want to receive traps for this entity at the severity levels you specified.

   (To move an entity name out of this column, select the entity name and then click on Remove.)

6. **Repeat Steps 2 through 5 for other slots you want to configure.**

7. **Click on Save.**

Configuring Exceptions

You can configure up to 50 exceptions, which specify that the SNMP agent always sends or never sends certain traps to the network management station regardless of the settings in the Trap Configuration window and regardless of slot.

To add an exception, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Trap Configuration→Exceptions.**

   The Traps Exceptions Lists window appears (Figure 1-15).

Figure 1-15. Traps Exceptions Lists Window

2. **Click on Add.**

   The Add Trap window appears (Figure 1-16).

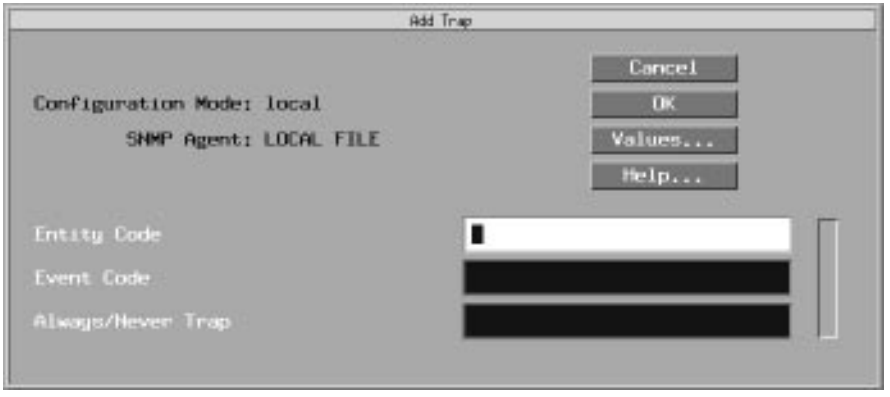


Figure 1-16. Add Trap Window

3. **Edit the parameters.**

   Use the descriptions that follow as a guide.

4. **Click on OK.**

Parameter:	**Entity Code**
Default:	None
Options:	Any valid entity code
Function:	Specifies the entity code for the event for which you want to configure an exception.
Instructions:	Enter the entity code of the event for which you want to configure an exception. Refer to the book *Event Messages for Routers and BNX Platforms* for entity codes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.6.1.3

Parameter:	**Event Code**
Default:	None
Options:	Any valid event code number
Function:	Specifies the code number for the event for which you want to configure an exception.
Instructions:	Enter the event code number for the event for which you want to configure an exception. Refer to the book *Event Messages for Routers and BNX Platforms* for event code numbers.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.6.1.4

Parameter:	**Always/Never Trap**
Default:	None
Options:	Always | Never
Function:	Specifies whether the SNMP agent always sends or never sends this trap to the network management station. The instructions you specify in this field override the settings in the Trap Configuration window, and affect traps sent from every slot in the router.
Instructions:	Select Always or Never.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.6.1.2

Deleting Exceptions

To delete an exception, begin at the Configuration Manager window (refer to Figure 1-3) and complete the following steps:

1. **Select Protocols→IP→SNMP→Trap Configuration→Exceptions.**

   The Traps Exceptions Lists window appears (refer to Figure 1-15).

2. **Select the trap for which you want to delete the exception.**

3. **Click on Delete.**

Chapter 2
Configuring BOOTP Services

Using Bootstrap (BOOTP) services, you can arrange for diskless clients to boot from a server on either their own or another (physical) network. Refer to this chapter for

- An overview of the BOOTP relay agent (see page 2-1)
- Features of the Bay Networks implementation of BOOTP (see page 2-5)
- Instructions for enabling BOOTP services (see page 2-7)
- Instructions for accessing and editing BOOTP parameters (see page 2-8)

BOOTP Relay Agent Overview

BOOTP allows a diskless client to boot remotely from a server on the same network or on a different physical network. The client broadcasts a request to boot from a remote server. When a suitable server receives the BOOTREQUEST packet, it responds to the client by issuing a BOOTREPLY packet. The server then transmits the boot file to the client via a transfer protocol, such as Trivial File Transfer Protocol (TFTP).

Figure 2-1 illustrates how BOOTP works when the client and the server are on the same network. The client transmits a BOOTREQUEST packet to the IP limited broadcast address (255.255.255.255). The server sends a BOOTREPLY packet to the client. Depending on the server's implementation, it addresses the packet to either the limited broadcast or the client's IP address.

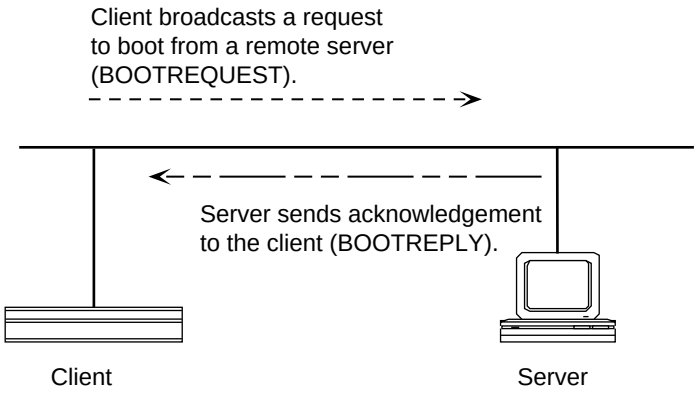


Figure 2-1. Client and Server on the Same Physical Network

If, however, the client and the server are on different physical networks, a BOOTP *relay agent* (also known as a BOOTP Gateway) must forward BOOTP packets to their correct destinations. When you configure a Bay Networks router for BOOTP services, the router acts as a BOOTP relay agent. Figure 2-2 illustrates how BOOTP works when the client and the server are on different physical networks.

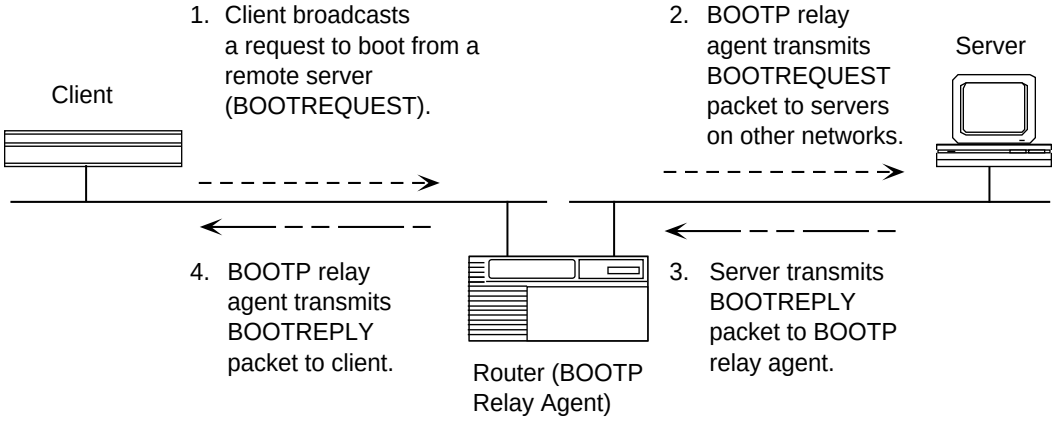


Figure 2-2. Client and Server on Different Physical Networks

The client transmits a BOOTREQUEST packet to the IP limited broadcast address (255.255.255.255). The router receives the BOOTREQUEST packet at an interface that you configured to receive BOOTREQUEST packets (an *input* interface). If the BOOTREQUEST packet has an address other than 255.255.255.255, the router drops the packet.

Figure 2-3 shows the fields in the BOOTREQUEST and BOOTREPLY packets.

<table>
<tr><td>Operation (1)*</td><td>Hardware type (1)</td><td>Hardware address length (1)</td><td>Hops (1)</td></tr>
<tr><td colspan="4">Transaction ID (4)</td></tr>
<tr><td colspan="2">Seconds (2)</td><td colspan="2">Flags (2)</td></tr>
<tr><td colspan="4">Client IP address (4)</td></tr>
<tr><td colspan="4">Your IP address (4)</td></tr>
<tr><td colspan="4">Server IP address (4)</td></tr>
<tr><td colspan="4">Gateway IP address (16)</td></tr>
<tr><td colspan="4">Client hardware address (16)</td></tr>
<tr><td colspan="4">Server name (64)</td></tr>
<tr><td colspan="4">File name (128)</td></tr>
<tr><td colspan="4">Vendor-specific area (64)</td></tr>
<tr><td colspan="4">* The number in parentheses indicates the number of octets in each field.</td></tr>
</table>

Figure 2-3. BOOTREQUEST and BOOTREPLY Fields

The packet relay process uses these fields as follows:

1. When a router interface receives a BOOTREQUEST packet, the router examines the *seconds* and *hops* fields in the packet and compares these values to BOOTP parameters you configured on that interface.

   The *seconds* field contains the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the value of the Timeout Secs. parameter you configured on the interface, the router drops the packet.

The *hops* field contains the maximum number of hops that a packet can take between the source and destination devices. If the packet has traversed more hops than the value of the hops parameter you specified for that interface, the router drops the packet.

2. If the router accepts the packet, it alters the packet by
   - Incrementing the *hops* field by 1
   - Writing the IP address of the input interface to the *gateway IP address* field
3. The router then determines which networks should receive this packet and broadcasts it to other networks through a forwarding route that you specify when you configure the router for BOOTP services.

   If the BOOTP packet has to travel to a network through another router, you must specify the forwarding route using one of the following methods:
   - Configure the second router for BOOTP services

     In this case, the second router inspects the packet in the same way as the first router, and increments the *hops* field by 1. The second router will not, however, replace the address in the *gateway IP address* field, since servers will reply to the first router that received the BOOTREQUEST packet
   - Configure the first router to forward the BOOTREQUEST packet to a specific server.

     In this case, the router will unicast the BOOTREQUEST packet to the server through normal IP services.
4. Servers on other networks receive the BOOTREQUEST packet and respond with a BOOTREPLY packet. Those servers transmit the BOOTREPLY packets through normal IP services to the address of the first interface that received the BOOTREQUEST packet. That address appears in the *gateway IP address* field in the BOOTREQUEST packet.
5. When the router that first received the BOOTREQUEST packet receives the BOOTREPLY packet, it examines the *gateway IP address* field to check that the value in this field is the same as the IP destination address that the server used for the packet. If the addresses differ, the router discards the BOOTREPLY packet.
6. If the router accepts the packet, it examines the *flag* field and forwards the packet to the client as follows:

- If the *flag* field contains the value 1, the client does not know its own IP address. The router broadcasts the BOOTREPLY packets to the IP limited broadcast address (255.255.255.255).
- If the *flag* field contains the value 0, the client knows its own IP address, which appears in the *client IP address* field of the BOOTREPLY packet. The router sends the BOOTREPLY packet to that IP address and the link-layer address that appears in the *client hardware address* field.

Implementation Notes

Bear the following issues in mind when you configure BOOTP services for the router.

Setting the Router Mode

You must configure the router in forwarding mode for the BOOTP relay agent to operate. For instructions on configuring the router in forwarding mode, refer to *Configuring IP Services*.

Specifying a Forwarding Route for BOOTREQUEST Packets

You must define forwarding routes for BOOTREQUEST packets, using one or both of the following methods:

- Defining a relationship between an input interface and an output interface on the router (refer to “Specifying Interfaces That Receive and Relay BOOTP Packets,” later in this chapter)
- Defining a relationship between an input interface and a BOOTP server (refer to “Specifying Servers for BOOTP Services,” later in this chapter)

Filtering BOOTP and DHCP Packets

The Dynamic Host Configuration Protocol (DHCP) also uses the BOOTP relay agent to forward packets. Refer to Chapter 3 for further information on DHCP. To reduce network traffic, you may want to control whether an interface transmits BOOTP packets, DHCP packets, or both BOOTP and DHCP packets. For example, you may want to set a filter to prevent BOOTP traffic from traversing a network segment that contains DHCP servers but not BOOTP servers.

You configure this type of filter by setting the Pass Through Mode parameter. This parameter appears in several windows you use to configure BOOTP services. The default setting is BOOTP and allows the interface to transmit only BOOTP packets. Be sure to change the setting if you want to transmit DHCP messages.

Improving the Efficiency of Packet Relay

You can improve the efficiency of the BOOTP packet relay process by

- Specifying the addresses of BOOTP servers
- Using traffic filters

Specifying BOOTP Servers

You specify a BOOTP server by assigning a particular BOOTP server to an output interface in the BOOT Relay Agent Preferred Server Table window (refer to Figure 2-9). For instructions about this procedure, refer to "Specifying Servers for BOOTP Services," later in this chapter.

In the BOOT Relay Agent Preferred Server Table window (refer to Figure 2-10), you enter the IP address of the input interface on the router and the IP address of the BOOTP server. The router can then unicast a BOOTREQUEST packet through normal IP services to that server.

Using Traffic Filters

For instructions on configuring traffic filters (not supported by BNX software), refer to *Configuring Traffic Filters and Protocol Prioritization.* The following example illustrates how you can use a traffic filter to enhance BOOTP operation.

Example

Consider a network segment that has two types of clients: one set that should boot using only servers on the local network and another set that should boot from remote servers. You could set up a traffic filter to drop any BOOTREQUEST packets from the first set, as follows:

- *Protocol:* User Datagram Protocol (UDP)
- *UDP destination port:* BOOTP server
- *User-defined field for the client hardware address in the BOOTP header:* all MAC addresses of clients in the local group

- *Action:* DROP

The user-defined field has the following attributes:

- *Reference:* after IP header
- *Offset*: 224 bits (7 longwords into the BOOTP header)
- *Length:* depends on the media (48 bits for LANs)

Using Unnumbered Interfaces

You can configure BOOTP services only on a numbered network interface. For instructions on numbering a network interface, refer to the book *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software.

Although you cannot configure an unnumbered interface to accept BOOTP requests, you can configure the router to transmit BOOTP requests from an unnumbered interface. To relay BOOTP packets through an unnumbered interface, you must specify an input interface on the router and a server in the BOOT Relay Agent Preferred Server Table window (refer to Figure 2-9). The router can then unicast a BOOTREQUEST packet through normal IP services to that server. For instructions about this procedure, refer to "Specifying Servers for BOOTP Services," later in this chapter.

Enabling BOOTP Services

This section describes how to enable IP and BOOTP services simultaneously. If you want to add BOOTP to a circuit on which you have already configured IP, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for information on adding a protocol.

When you enable BOOTP services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

This section assumes that you have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, and that you have

1. Opened a configuration file
2. Specified router hardware if this is a local mode configuration file

3. Selected the link or net module connector on which you are enabling IP services, or configured a WAN circuit if this connector requires one

Enabling BOOTP on an Interface

When you select a link or net module connector, or when you finish configuring a WAN circuit, the Select Protocols window appears (refer to Figure 1-1).

Note: *The window varies slightly according to circuit type, displaying only those protocols that the circuit type supports.*

To enable BOOTP on an interface:

1. **Select BOOTP from the Select Protocols menu.**

   When you select BOOTP, you automatically select IP.

2. **Click on OK.**

   The IP Configuration window appears (refer to Figure 1-2).

3. **Edit the parameters on the screen.**

   Refer to "Enabling IP on an Interface" in Chapter 1 for guidelines.

4. **Edit or accept the default values for the remaining IP interface parameters, as follows:**

   - **To accept the default values, click on OK.**

   Site Manager displays the Configuration Manager window. You can now customize BOOTP parameters for the IP interface (refer to "Accessing BOOTP Parameters").

   - **To edit all IP interface parameters, click on Details.**

   Refer to *Configuring IP Services* for information about editing IP interface parameters.

Accessing BOOTP Parameters

Use the Configuration Manager to edit BOOTP parameters for IP interfaces. You access all BOOTP parameters from the Configuration Manager window (refer to Figure 1-3). Refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for instructions on accessing this window.

For each BOOTP parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object OID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software.*

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

Editing BOOTP Relay Agent Parameters

To edit BOOTP relay agent parameters, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→BOOTP→Relay Agent Interface Table.**

   The BOOTP Relay Agent Interface Table window appears (Figure 2-4). This window lists all the IP interfaces that you have configured for BOOTP services on the router.

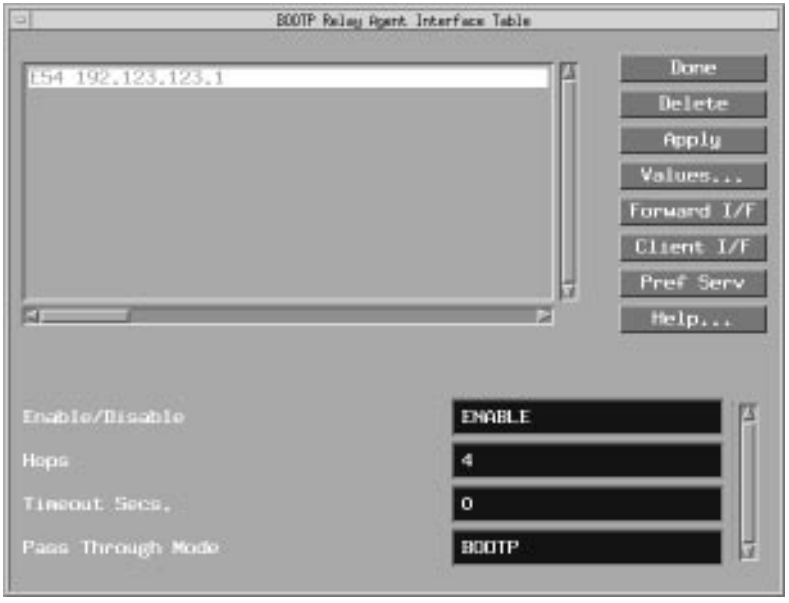


Figure 2-4. BOOTP Relay Agent Interface Table Window

2. **Click on the interface for which you want to edit BOOTP parameters.**
3. **Edit the parameters you want to change.**

   Use the descriptions that follow as a guide.
4. **Click on Apply to implement your changes.**

   You can also perform the following procedures from this window:
5. **Click on Done to exit the window.**

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether BOOTP is active on the network interface.
Instructions:	Select Enable to enable BOOTP on the network interface. Select Disable to disable BOOTP on the network interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.1.1.2

Parameter:	**Hops**
Default:	4
Range:	1 to 16 hops
Function:	Specifies the maximum number of hops from the client to the server. A hop is the logical distance between two devices. If the value in the *hops* field of a BOOTREQUEST packet is greater than the number you specify for this parameter, the router drops the packet.
Instructions:	Accept the default of 4 hops or specify a number between 1 and 16, inclusive.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.1.1.5

Parameter:	**Timeout Secs.**
Default:	0 second
Range:	0 to 65535 seconds
Function:	Specifies the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the *seconds* field of a BOOTREQUEST packet is less than the value you specify for this parameter, the router drops the packet.
Instructions:	Accept the default, 0, or specify a number between 1 and 65535, inclusive.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.1.1.6

Parameter:	**Pass Through Mode**
Default:	BOOTP
Options:	BOOTP | DHCP | BOOTP and DHCP
Function:	Specifies whether the interface relays BOOTP, DHCP, or BOOTP and DHCP requests
Instructions:	Select BOOTP to relay BOOTP requests. Select DHCP to relay DHCP requests. Select BOOTP and DHCP to relay both BOOTP and DHCP requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.1.1.16

Specifying Interfaces That Receive and Relay BOOTP Packets

You must specify a forwarding route for BOOTREQUEST packets. You can do so by defining a relationship between an interface you want to receive BOOTREQUEST packets and an interface you want to transmit BOOTREQUEST packets. When you define this type of relationship, the interface pair appears in the BOOTP Relay Agent Forwarding Table window.

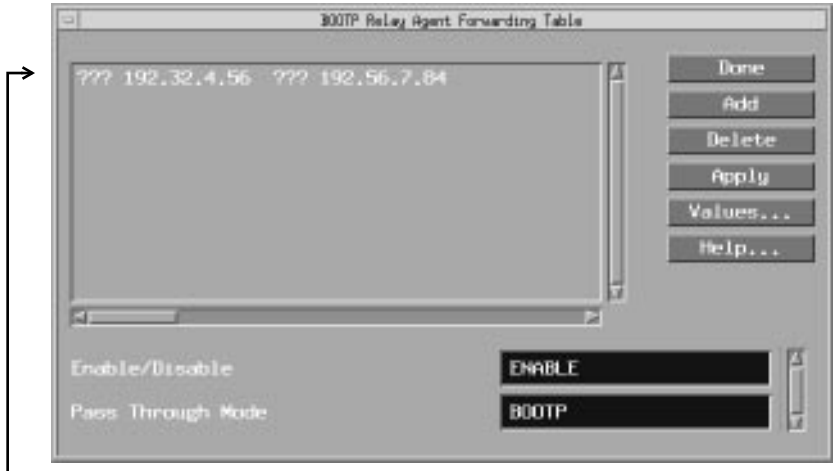
Depending on the configuration of your network, you can specify

- One input IP interface to forward packets to multiple output IP interfaces
- Multiple input interfaces to forward to multiple output interfaces
- Multiple input interfaces to forward to one output interface

To create the BOOTP relay agent forwarding table, begin at the BOOTP Relay Agent Interface Table window (refer to Figure 2-4) and proceed as follows:

1. **Click on Forward I/F.**

   The BOOTP Relay Agent Forwarding Table window appears (Figure 2-5).



??? means that you have not configured the IP interface on the router

Figure 2-5. BOOTP Relay Agent Forwarding Table Window

2. **Click on Add.**

   The BOOTP Addresses window appears (Figure 2-6).

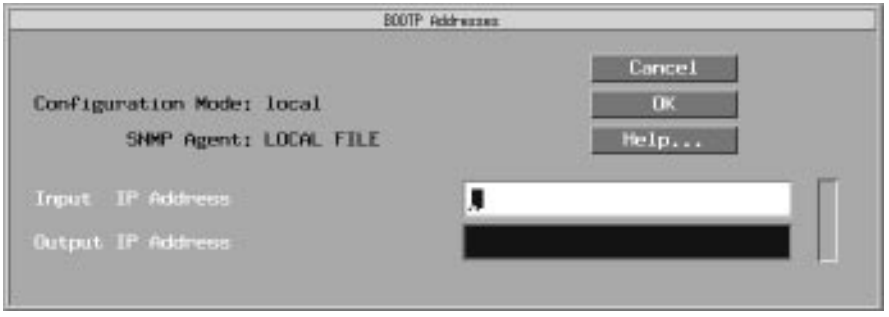


Figure 2-6. BOOTP Addresses Window

3. **Specify the input IP and output IP addresses.**

   Use the descriptions that follow as a guide.

4. **Click on OK.**

   The BOOTP Relay Agent Forwarding Table window now lists the interface pair you added and default values for the Enable/Disable and Pass Through Mode parameters. Note that if you entered an IP address that you have not configured on the router, `???` appears before the IP address (example: `??? 111.111.111.111`). When you configure the IP address on the router, Site Manager replaces `???` with the appropriate address.

5. **Edit the Enable/Disable and Pass Through Mode parameters, if you want.**

   Use the descriptions that follow as a guide.

6. **Click on Done to exit the window.**

Parameter:	**Input IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP interface that receives BOOTREQUEST packets from clients.
Instructions:	Enter the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients, then configure this IP address on the router, if you have not already done so. Do not specify an unnumbered interface for this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.3

Parameter:	**Output IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP interface that forwards BOOTREQUEST packets to an external network.
Instructions:	Enter the IP address of a numbered network interface that you want to transmit BOOTREQUEST or DHCP packets to servers, then configure this IP address on the router, if you have not already done so. Do not specify an unnumbered interface for this parameter. If you want to use an unnumbered interface to transmit BOOTREQUEST or DHCP packets to servers, you must set up a preferred server from the BOOTP Relay Agent Interface Table window.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.4

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this forwarding route is active.
Instructions:	Select Enable to allow BOOTP or DHCP forwarding through this route. Select Disable to prevent BOOTP or DHCP forwarding through this route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.2

Parameter:	**Pass Through Mode**
Default:	BOOTP
Options:	BOOTP | DHCP | BOOTP and DHCP
Function:	Specifies whether the interface relays BOOTP, DHCP, or BOOTP and DHCP requests.
Instructions:	Select BOOTP to relay BOOTP requests.
	Select DHCP to relay DHCP requests.
	Select BOOTP and DHCP to relay both BOOTP and DHCP requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.1.5

Deleting an Input/Output Address Pair

To delete an input/output address pair, begin at the BOOTP Relay Agent Forwarding Table window (refer to Figure 2-5) and proceed as follows:

1. **Click on the address pair to select it.**
2. **Click on Delete.**

   The BOOTP Relay Agent Forwarding Table window no longer displays the address pair.
3. **Click on Done to exit the window.**

Configuring an AN to Use EZ-Install over a Frame Relay PVC

You must create a BOOTP *client interface table* if you intend to configure an Access Node (AN) to use EZ-Install over a Frame Relay permanent virtual circuit (PVC) in group access mode. You do not need to create this table if you configured the Frame Relay PVC to operate in direct access mode.

The BOOTP client interface table allows you to pair the IP address of a remote AN that will boot via EZ-Install with the local Data Link Connection Identifier (DLCI) of its Frame Relay group access PVC.

For information about configuring an AN to use EZ-Install, refer to *Installing and Starting AN Routers*. For information about DLCI and Frame Relay, refer to *Configuring Frame Relay Services*.

To create the BOOTP client interface table, begin at the BOOTP Relay Agent Interface Table window (refer to Figure 2-4) and proceed as follows:

1. **Click on Client I/F.**

   The BOOTP Client Interface Table window appears (Figure 2-7).

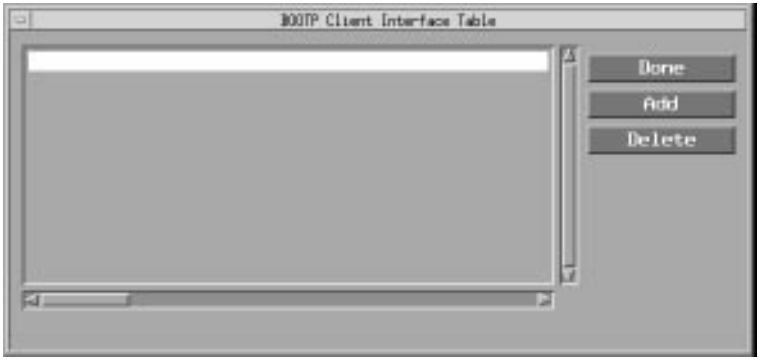


Figure 2-7. BOOTP Client Interface Table Window

2. **Click on Add.**

   The BOOTP Client Interface Address window appears (Figure 2-8).

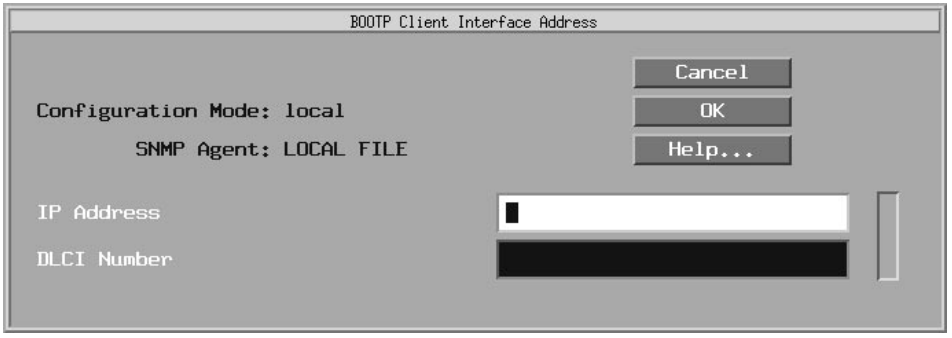


Figure 2-8. BOOTP Client Interface Address Window

3. **Enter values for the IP Address and DLCI Number parameters.**

   Use the descriptions that follow as a guide.

4. **Click on OK.**

   The BOOTP Client Interface Table window now lists the client IP interface and the DLCI number you added.

5. **Click on Done to exit the window.**

Parameter:	**IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP address of the remote AN that will boot using EZ-Install over a Frame Relay group access PVC connection to the router.
Instructions:	Enter the IP address of the remote AN.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.1.1.1.3

Parameter:	**DLCI Number**
Default:	None
Range:	16 to 1007
Function:	Specifies the Frame Relay PVC identification number whose destination is the remote AN that will boot using EZ-Install. The Frame Relay network uses the DLCI number to direct data flow.
Instructions:	Enter the DLCI number, in decimal format, for the group access PVC to the remote AN. Use the DLCI number assigned by your Frame Relay service provider.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.1.1.1.2

Specifying Servers for BOOTP Services

You must specify a forwarding route for BOOTREQUEST packets. You can do so by defining a relationship between an input interface and a BOOTP server. By defining such a relationship, you can

- Improve the efficiency of BOOTREQUEST packet relay
- Transmit BOOTREQUEST packets through unnumbered output interfaces

To specify servers for BOOTP services:

1. **Click on Pref Serv in the BOOTP Relay Agent Interface Table window (refer to Figure 2-4).**

   The BOOTP Relay Agent Preferred Server Table window appears (Figure 2-9).

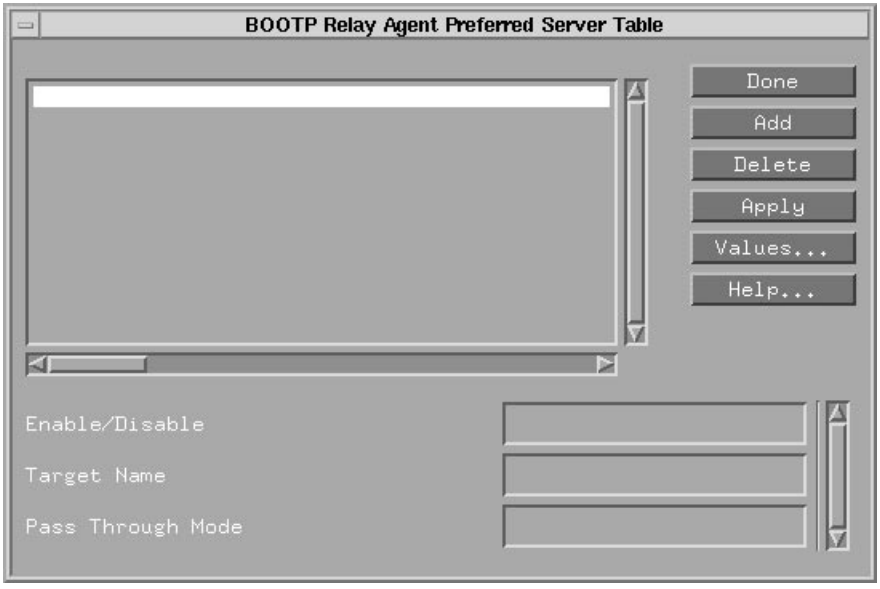


Figure 2-9. BOOTP Relay Agent Preferred Server Table Window

2. **Click on Add.**

   The BOOTP Preferred Server Configuration window appears (Figure 2-10).

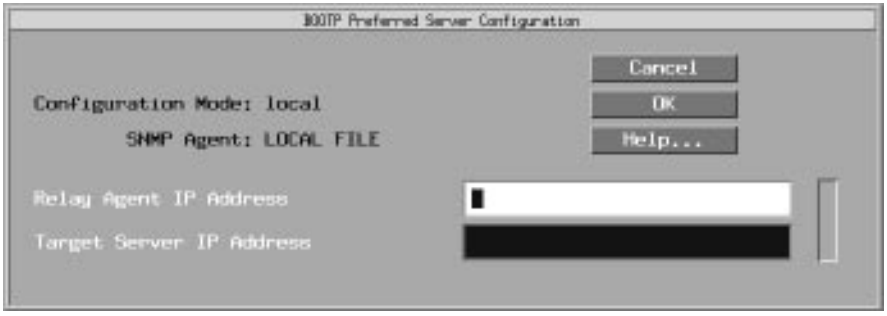


Figure 2-10. BOOTP Preferred Server Configuration Window

3. **Enter values for the Relay Agent IP Address and the Target Server IP Address parameters.**

   Use the descriptions that follow as a guide.

4. **Click on OK.**

   The BOOTP Relay Agent Preferred Server Table window now shows the address pair you added and default values for the Enable/Disable and Pass Through Mode parameters.

5. **Edit the Enable/Disable and Pass Through Mode parameters, if you want.**

   Use the descriptions that follow as a guide.

6. **Click on Done to exit the window.**

Parameter:	**Relay Agent IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP interface that receives BOOTREQUEST packets from clients.
Instructions:	Enter the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients, then configure this IP address on the router, if you have not already done so. Do not specify an unnumbered interface for this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.3.1.3

Parameter:	**Target Server IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the address of a server that should receive BOOTREQUEST or DHCP packets.
Instructions:	Enter the IP address of the server that should receive the BOOTREQUEST or DHCP packet.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.3.1.4

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the forwarding route is active.
Instructions:	Select Enable to allow BOOTP or DHCP forwarding through this route. Select Disable to prevent BOOTP or DHCP forwarding through this route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.3.1.2

Parameter:	**Target Name**
Default:	None
Options:	Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces.
Function:	Specifies the target server's host name.
Instructions:	If you want to keep track of the names of BOOTP or DHCP servers, enter the target server's host name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.3.1.5

Parameter:	**Pass Through Mode**
Default:	BOOTP
Options:	BOOTP | DHCP | BOOTP and DHCP
Function:	Specifies whether the interface relays BOOTP, DHCP, or BOOTP and DHCP requests
Instructions:	Select BOOTP to relay BOOTP requests. Select DHCP to relay DHCP requests. Select BOOTP and DHCP to relay both BOOTP and DHCP requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.3.1.6

Deleting the BOOTP Relay Agent from an IP Interface

To delete a BOOTP relay agent, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→BOOTP→Relay Agent Interface Table.**

   The BOOTP Relay Agent Interface Table window appears (refer to Figure 2-4).

2. **Click on the interface from which you want to delete BOOTP.**

3. **Click on Delete.**

   This action deletes the BOOTP relay agent and all of the forwarding table entries that you specified from the selected interface.

Deleting BOOTP Globally

To globally delete BOOTP on the router, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→BOOTP→Delete.**

2. **Click on Delete.**

   This action deletes BOOTP from all interfaces on the router.

Chapter 3
Configuring DHCP Services

Using Dynamic Host Configuration Protocol (DHCP), you can enable clients to acquire permanent IP configuration parameters and a temporary IP address. Refer to this chapter for

- An overview of the DHCP protocol (see page 3-1)
- Features of the Bay Networks implementation of DHCP (see page 3-6)
- Instructions for enabling DHCP services (see page 3-6)
- Instructions for accessing and editing DHCP parameters (see page 3-7)

DHCP Overview

DHCP enables clients to obtain an IP address for a fixed length of time (a *lease period*) from remote servers (*DHCP servers*). The lease period can range from 1 minute to 99 years. When the lease period expires, the server can assign the IP address to another client on the network. DHCP also enables clients to acquire the IP configuration parameters they need to communicate on a network.

DHCP uses the BOOTP relay agent to forward packets. The BOOTP relay agent uses the same criteria and methods for forwarding both DHCP and BOOTP packets. Refer to “BOOTP Relay Agent Overview” in Chapter 2 for information about the packet relay process.

Acquiring a New IP Address and New Configuration Parameters

This process involves the following stages:

- Identifying DHCP servers
- Requesting IP information
- Receiving IP information
- Accepting IP information

Figure 3-1 shows the first stage of the process.

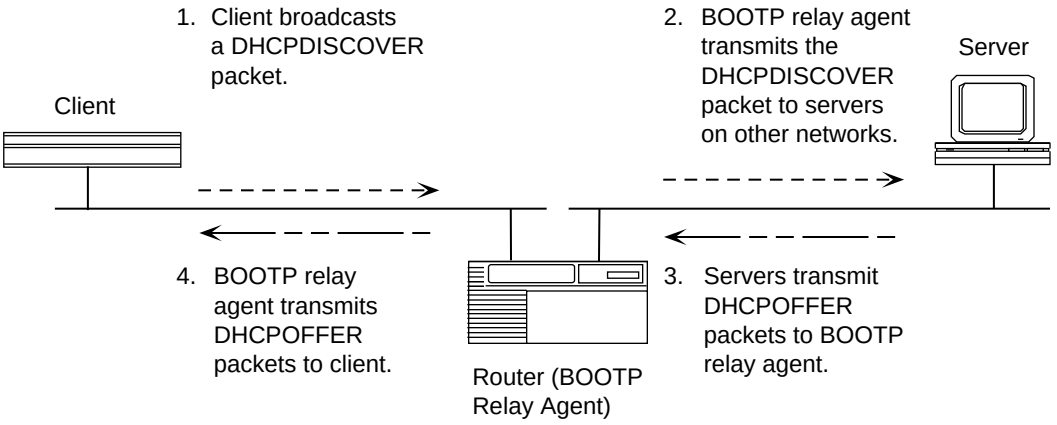

1. Client broadcasts a DHCPDISCOVER packet.
2. BOOTP relay agent transmits the DHCPDISCOVER packet to servers on other networks.
Server
Client
4. BOOTP relay agent transmits DHCPOFFER packets to client.
3. Servers transmit DHCPOFFER packets to BOOTP relay agent.
Router (BOOTP Relay Agent)

Figure 3-1. Identifying DHCP Servers

To identify DHCP servers, the client broadcasts a DHCPDISCOVER packet. Figure 3-2 shows the fields in a DHCP packet. The packet relay process uses these fields as follows:

1. A BOOTP relay agent receives the packet, and if it accepts the packet, transmits the packet to DHCP servers on other networks.

Operation (1)*	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction ID (4)			
Seconds (2)		Flags (2)	
Client IP address (4)			
Your IP address (4)			
Server IP address (4)			
Gateway IP address (16)			
Client hardware address (16)			
Server name (64)			
File name (128)			
Options (312)			
* The number in parentheses indicates the number of octets in each field.			

Figure 3-2. Fields in a DHCP Packet

2. Those servers may respond with a DHCPOFFER packet that includes an available IP address in the *your IP address* field.

   When a DHCP server offers an IP address, that address is temporarily unavailable to other clients. If the client does not accept or reject the address within a certain period of time, the server reclaims it. The address is then available for other clients.

3. The BOOTP relay agent receives the DHCPOFFER packet and examines the packet. If the BOOTP relay agent accepts the packet, it forwards it to the client.

4. If a client does not receive a DHCPOFFER packet within a certain amount of time after broadcasting a DHCPDISCOVER packet, it sends the packet again. The client will rebroadcast the packet up to 10 times.

   The client may receive DHCPOFFER packets from several potential servers. If you configure the client to wait for multiple responses, it compares configuration parameters in the DHCPOFFER packets to decide which server to target.

Figure 3-3 shows the second and third stages of the process.

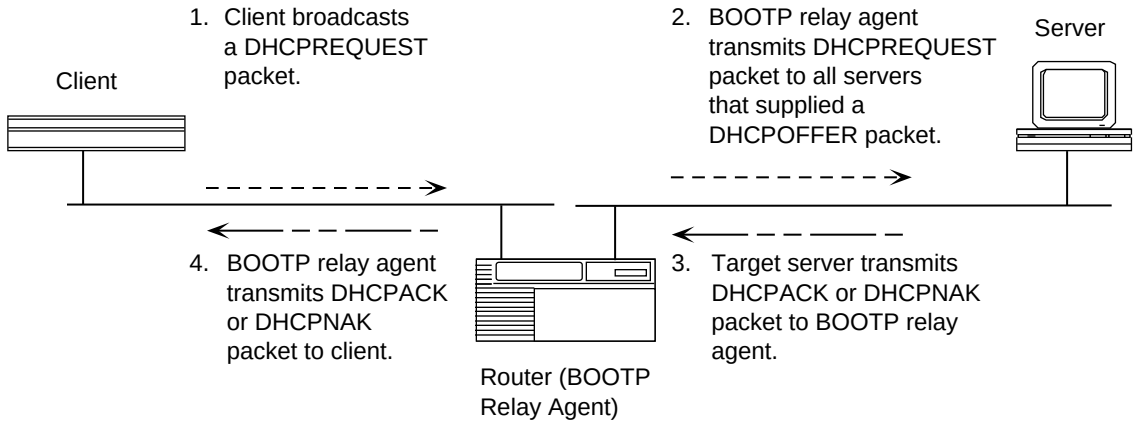

1. Client broadcasts a DHCPREQUEST packet.
2. BOOTP relay agent transmits DHCPREQUEST packet to all servers that supplied a DHCPOFFER packet.
Server
Client
4. BOOTP relay agent transmits DHCPACK or DHCPNAK packet to client.
3. Target server transmits DHCPACK or DHCPNAK packet to BOOTP relay agent.
Router (BOOTP Relay Agent)

Figure 3-3. Requesting and Receiving IP Information

5. When the client has chosen a target server, it broadcasts a DHCPREQUEST packet. The DHCPREQUEST packet contains the address of the target server in the *server IP address* field.
6. The router receives the packet and forwards it to all servers.
7. Those servers examine the packet, and if their IP addresses differ from the value in the *server IP address* field, they reclaim the IP addresses they supplied in the DHCPOFFER packets. These addresses are now available for other clients.
8. The target server recognizes its IP address in the *server IP address* field, and responds to the DHCPREQUEST packet as follows:
   - If the target server can supply the requested configuration parameters, it sends a DHCPACK packet to the client through the BOOTP relay agent.

     The client examines the configuration parameters in the DHCPACK packet and records the duration of the lease period. If the client detects a problem with the configuration parameters, it sends a DHCPDECLINE packet to the server and issues a new DHCPDISCOVER packet. Otherwise, the client accepts the configuration parameters.

- If the target server cannot supply the requested configuration parameters, it sends a DHCPNAK packet to the client through the BOOTP relay agent.

  When the client receives the DHCPNAK packet, it broadcasts a new DHCPDISCOVER packet and the process begins again.

A client may choose to relinquish its IP address before the lease period expires by sending a DHCPRELEASE packet to the server. A DHCPRELEASE packet contains the relinquished IP address in the *client IP address* field and the client's MAC address in the *client hardware address* field.

Acquiring the Same IP Address Again

A client may want to reuse an IP address that a server allocated earlier by DHCP or any other method. In this case, the interchange between client and server omits some of the steps described in the previous section, and proceeds as follows:

1. The client starts the interchange by broadcasting a DHCPREQUEST packet that contains its previous IP address in the *client IP address* field.
2. The BOOTP relay agent forwards the packet to DHCP servers on other networks.
3. DHCP servers examine the client's configuration parameters in the *options* field of the DHCPREQUEST packet.
4. The server that originally supplied the configuration parameters recognizes them and responds with a DHCPACK packet.
5. When a client receives a DHCPACK packet, it accepts or declines the parameters, as it would when receiving a new IP address.

If a client's request is invalid (for example, if the client has moved to a new network), servers respond with a DHCPNAK packet. If a client receives only DHCPNAK packets, it must request a new IP address by broadcasting a DHCPDISCOVER packet.

Implementation Notes

DHCP uses the BOOTP relay agent to forward packets. When implementing DHCP on a router, you need to consider the same issues you would consider when implementing BOOTP services. Refer to "Implementation Notes" in Chapter 2 for full details.

Enabling DHCP Services

This section describes how to enable IP, BOOTP, and DHCP services simultaneously. If you want to add BOOTP and DHCP to a circuit on which you have already configured IP, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for information on adding a protocol.

When you enable these services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

This section assumes that you have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, and that you have

1. Opened a configuration file
2. Specified router hardware if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling IP services, or configured a WAN circuit if this connector requires one

Enabling DHCP on an Interface

When you select a link or net module connector, or when you finish configuring a WAN circuit, the Select Protocols window appears (refer to Figure 1-1).

Note: *The window varies slightly according to circuit type, displaying only those protocols that the circuit type supports.*

For each DHCP parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software.*

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

To enable DHCP on an interface, complete the following steps:

1. **Enable BOOTP on the interface.**

   Refer to "Enabling BOOTP on an Interface" in Chapter 2 for instructions.

2. **Access the BOOTP Relay Agent Interface Table window (refer to Figure 2-4).**

   Refer to "Editing BOOTP Relay Agent Parameters" in Chapter 2 for instructions.

3. **Set the Pass Through Mode parameter to DHCP, or BOOTP and DHCP.**

4. **Click on Apply.**

   This action allows you to select DHCP or BOOTP and DHCP for the Pass Through Mode parameter in other windows.

5. **Edit the other parameters in this window.**

   Refer to "Editing BOOTP Relay Agent Parameters" in Chapter 2 for guidelines.

Accessing and Editing DHCP Parameters

When you have enabled DHCP services on a router, you can configure the router software for your specific requirements. Use the remaining sections in this chapter as a guide.

Specifying Interfaces That Receive and Relay DHCP Packets

You must specify a forwarding route for DHCP packets. You can do so by defining a relationship between an interface you configured to receive DHCP packets and an interface you want to transmit DHCP packets.

When you define this type of relationship, the interface pair appears in the BOOTP relay agent forwarding table. Refer to “Specifying Interfaces That Receive and Relay BOOTP Packets” in Chapter 2 for instructions.

Be sure to set the Pass Through Mode parameter in the BOOTP Relay Agent Forwarding Table window (refer to Figure 2-5) to DHCP, or BOOTP and DHCP, to allow DHCP operation.

Specifying Servers for DHCP Services

You can improve the efficiency of the packet forwarding process or transmit DHCP packets through unnumbered interfaces by specifying servers for DHCP services. Refer to “Specifying Servers for BOOTP Services” in Chapter 2 for instructions.

Be sure to set the Pass Through Mode parameter in the BOOTP Relay Agent Preferred Server Table window (refer to Figure 2-9) to DHCP, or BOOTP and DHCP, to allow DHCP operation.

Deleting DHCP from an IP Interface

To delete DHCP from an IP interface, while maintaining BOOTP on that interface, set the Pass Through Mode parameter in the BOOTP Relay Agent Interface Table window (refer to Figure 2-4) to BOOTP.

To delete both DHCP and BOOTP from an IP interface, delete the BOOTP relay agent on that interface. Refer to “Deleting the BOOTP Relay Agent from an IP Interface” in Chapter 2 for instructions.

Deleting DHCP Globally

To delete DHCP globally, you must delete BOOTP globally. Refer to “Deleting BOOTP Globally” in Chapter 2 for instructions.

Chapter 4
Configuring RARP Services

You can use a Bay Networks router as a Reverse Address Resolution Protocol (RARP) server that assigns IP addresses to its clients on the local area network. To configure a router as a RARP server, refer to the following information in this chapter:

- An overview of the RARP protocol (see page 4-1)
- Enabling RARP services (see page 4-2)
- Accessing and editing RARP parameters (see page 4-3)

RARP Overview

When you configure a router to use RARP services, it acts as a RARP server. A RARP server supplies clients on the same physical or logical LAN with IP addresses (Figure 4-1).

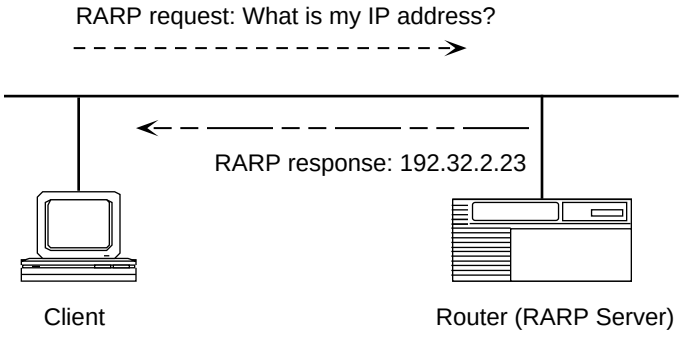


Figure 4-1. RARP Server Supplying an IP Address

To use RARP services, you must set up a *MAC address-to-IP address mapping table*. This table lists the MAC addresses of clients and the corresponding IP addresses that the RARP server should assign to those clients. When a client needs to acquire an IP address, the following interchange takes place:

1. The client broadcasts a RARP request specifying its MAC address.
2. Upon receiving a RARP request, the router refers to its MAC address-to-IP address mapping table, then sends the client a response packet containing the corresponding IP address.
3. The client examines the response packet to learn its IP address.

You can configure RARP support on Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) interfaces.

Enabling RARP Services

This section describes how to enable IP and RARP services simultaneously. If you want to add RARP to a circuit on which you have already configured IP, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for information on adding a protocol.

When you enable RARP services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

This section assumes that you have read *Configuring Routers* or *Configuring Customer Access (BNX Software)*, depending on the type of installed software, and that you have

1. Opened a configuration file
2. Specified router hardware if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling IP services, or configured a WAN circuit if this connector requires one

Enabling RARP on an Interface

When you select a link or net module connector, or when you finish configuring a WAN circuit, the Select Protocols window appears (refer to Figure 1-1).

Note: *The window varies slightly according to circuit type, displaying only those protocols that the circuit type supports.*

To enable RARP on an interface:

1. **Select Reverse ARP from the Select Protocols menu.**

   When you select RARP, you automatically select IP.

2. **Click on OK.**

   The IP Configuration window appears (refer to Figure 1-2).

3. **Edit the parameters on the screen.**

   Refer to "Enabling IP on an Interface" in Chapter 1 for guidelines.

4. **Edit or accept the default values for the remaining IP interface parameters, as follows:**

   - **To accept the default values, click on OK.**

   Site Manager displays the Configuration Manager window. You can now customize RARP parameters for the IP interface (refer to "Accessing RARP Parameters").

   - **To edit all IP interface parameters, click on Details.**

   Refer to *Configuring IP Services* for information about editing IP interface parameters.

Accessing RARP Parameters

The remaining sections in this chapter describe how to use the Configuration Manager to edit RARP parameters.

Note: *The instructions in this section assume that you have already configured at least one IP interface on which you have enabled RARP. If you have not yet configured an IP interface, or want to add additional IP interfaces, refer to "Enabling RARP Services" for instructions.*

You access all RARP parameters from the Configuration Manager window (refer to Figure 1-3). See *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for instructions on accessing this window.

For each RARP parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software.*

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

Disabling and Re-Enabling RARP Interfaces

To disable or re-enable individual RARP interfaces, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→Reverse ARP→Interface Table.**

   The RARP Interface Table window appears (Figure 4-2).

   This window lists all RARP interfaces configured on the router.

2. **Click on the RARP interface you want to select from the list of interfaces.**
3. **Set the Enable/Disable parameter.**

   Use the descriptions that follow as a guide.

4. **Click on Apply to implement your change.**
5. **Click on Done to exit the window.**

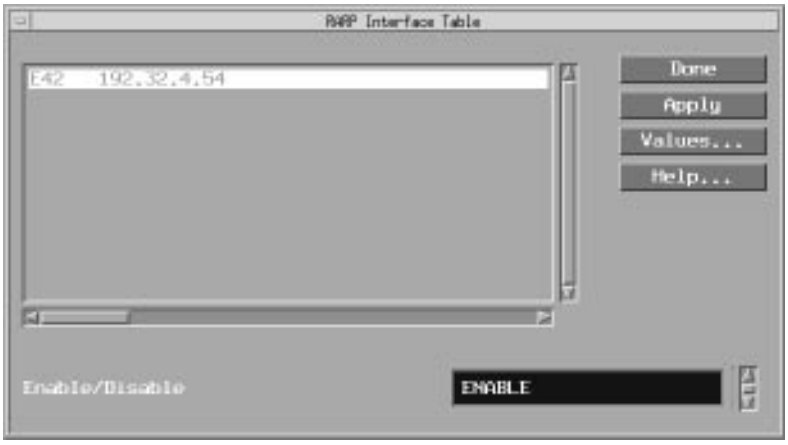


Figure 4-2. RARP Interface Table Window

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Re-enables or disables the RARP interface you selected from the list of interfaces.
Instructions:	Select Enable to re-enable a disabled interface.
	Select Disable to disable an interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.9.3.1.2

Defining the RARP Mapping Table

To define the router's MAC address-to-IP address RARP mapping table, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→Reverse ARP→Map Table.**

   The RARP Map Table window appears (Figure 4-3).

   This window lists the clients on the network that can use the router's RARP services.

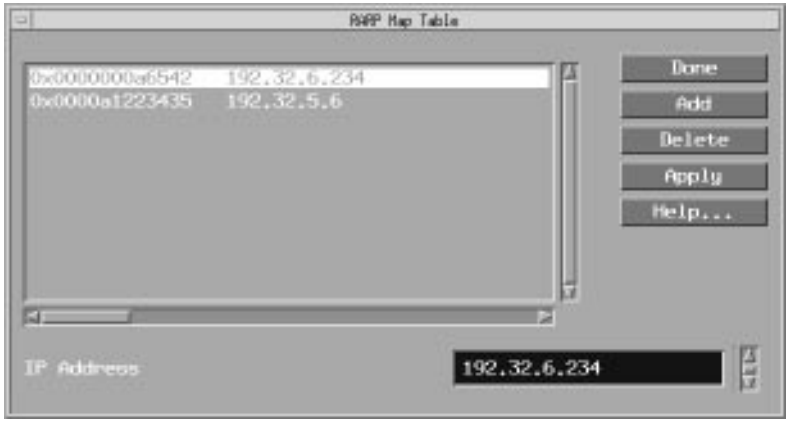


Figure 4-3. RARP Map Table Window

2. **Click on Add to add a new entry to the table.**

   The RARP Addresses window appears (Figure 4-4).

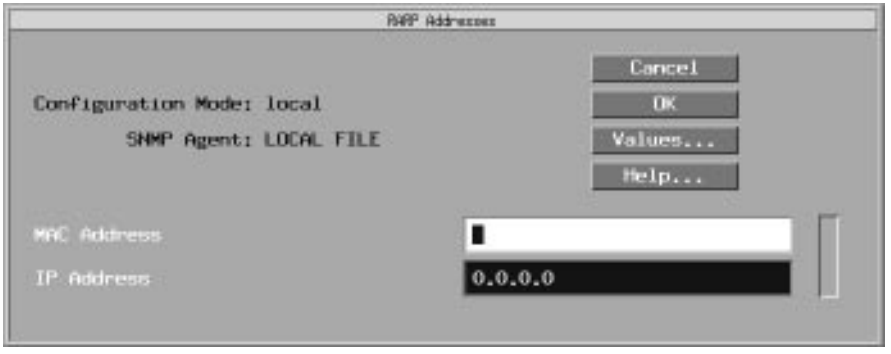


Figure 4-4. RARP Addresses Window

3. **Specify a MAC address and a corresponding IP address for the client.**

   Use the descriptions that follow as a guide.

4. **Click on OK.**

   The RARP Map Table window now displays the entry you defined.

5. **Click on Done to exit the window.**

Parameter:	**MAC Address**
Default:	None
Options:	Any valid MAC address
Function:	Specifies the MAC address of a client that will use the RARP services of this router. The client will include the MAC address you specify here in RARP requests it broadcasts to the router.
Instructions:	Enter the MAC address of a client.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.9.2.1.2

Parameter:	**IP Address**
Default:	0.0.0.0
Options:	Any valid IP address
Function:	Specifies the corresponding IP address for the client with the MAC address you specify. When the router receives a RARP request from the client, the router assigns this IP address to the client and includes it in a response packet.
Instructions:	Enter the IP address corresponding to the value of the MAC Address parameter. Do not accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.9.2.1.3

Disabling RARP Globally

To globally disable RARP from all router interfaces on which it is configured, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→Reverse ARP→Globals.**

   The Edit RARP Global Parameters window appears (Figure 4-5).

Figure 4-5. Edit RARP Global Parameters Window

2. **Set the Enable/Disable parameter to Disable.**
3. **Click on OK.**

   This action disables RARP on all router interfaces.

Deleting RARP Globally

To globally delete RARP from all router interfaces on which it is configured, begin at the Configuration Manager window (refer to Figure 1-3) and proceed as follows:

1. **Select Protocols→IP→Reverse ARP→Delete RARP.**

   The following confirmation window appears (Figure 4-6).

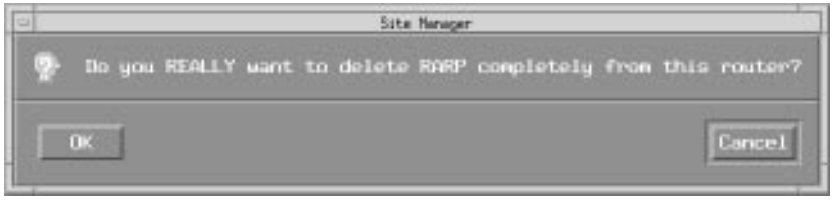


Figure 4-6. Confirmation Window for Deleting RARP

2. **Click on OK.**

   This action deletes RARP from all interfaces on the router.

Appendix A
Default Parameter Settings

SNMP Parameters

Tables A-1 through A-6 list the Site Manager default parameter settings for SNMP.

Table A-1. SNMP Global Parameters

Parameter	Default
Enable	Enable
Use Lock	Enable
Lock TimeOut	2 minutes
Authentication Failure Traps	Enable

Table A-2. SNMP Community Parameters

Parameter	Default
Community Name	None
Access	Read Only

Table A-3. SNMP Manager Parameters

Parameter	Default
Trap Port	162
Trap Types	Generic

Table A-4. SNMP Threshold Global Parameters

Parameter	Default
Polling Interval	60 s

Table A-5. SNMP Threshold Interface Parameters

Parameter	Default
Threshold Enable	Enable
Threshold Low Value	0
Threshold Low Event Level	Info
Threshold Medium Value	0
Threshold Medium Event Level	Info
Threshold High Value	0
Threshold High Event Level	Info
Threshold Units	Persecond
Threshold Action	Greaterthan
Threshold Max Successive Alarms	5
Threshold HoldDown Intervals	1
Threshold Label	ASN.1 object identifier

Table A-6. SNMP Trap Interface Parameters

Parameter	Default
Entity Code	None
Event Code	None
Always/Never Trap	None

BOOTP and DHCP Parameters

Tables A-7 through A-10 list the Site Manager default parameter settings for BOOTP and DHCP.

Table A-7. BOOTP Relay Agent Interface Parameters

Parameter	Default
Enable/Disable	Enable
Hops	4
Timeout Secs.	0 s
Pass Through Mode	BOOTP

Table A-8. BOOTP Addresses Parameters

Parameter	Default
Input IP Address	None
Output IP Address	None
Enable/Disable	Enable
Pass Through Mode	BOOTP

Table A-9. BOOTP Client Interface Address Parameters

Parameter	Default
IP Address	None
DLCI Number	None

Table A-10. BOOTP Preferred Server Configuration Parameters

Parameter	Default
Relay Agent IP Address	None
Target Server IP Address	None
Target Name	None
Enable/Disable	Enable
Pass Through Mode	BOOTP

RARP Parameters

Tables A-11 and A-12 list the Site Manager default parameter settings for RARP.

Table A-11. RARP Interface Parameters

Parameter	Default
Enable/Disable	Enable

Table A-12. RARP Address Parameters

Parameter	Default
MAC Address	None
IP Address	0.0.0.0

Index

A

Access parameter, 1-26

accessing parameters
- BOOTP, 2-8
- DHCP, 3-7
- RARP, 4-3
- SNMP, 1-20

adding
- entries to the RARP mapping table, 4-5
- SNMP communities, 1-24
- SNMP managers, 1-27
- *See also* configuring

Always/Never Trap parameter, 1-43

Authentication Failure Traps parameter, 1-23

B

BOOTP
- client interfaces table, creating, 2-15
- forwarding table, creating, 2-11
- gateway, 2-1
- implementation notes for, 2-5 to 2-7
- interfaces, assigning, 2-5
- overview of protocol, 2-1
- packet, 2-1 to 2-4, 2-5
- parameters. *See* BOOTP parameters
- relay agent, 2-2, 3-2
  - creating forwarding table for, 2-11
- servers, configuring, 2-6
- services, enabling, 2-7

BOOTP parameters
- addresses
  - Enable/Disable, 2-14
  - Input IP Address, 2-13
  - Output IP Address, 2-14
  - Pass Through Mode, 2-15
- client interface address
  - DLCI Number, 2-17
  - IP Address, 2-17
- defaults, A-3 to A-4
- preferred server
  - Enable/Disable, 2-20
  - Pass Through Mode, 2-21
  - Relay Agent IP Address, 2-20
  - Target Server IP Address, 2-20
- relay agent interface
  - Enable/Disable, 2-10
  - Hops, 2-10
  - Pass Through Mode, 2-11
  - Timeout Secs., 2-11

Bootstrap protocol. *See* BOOTP

C

Community Name parameter, 1-25

configuring
- BOOTP parameters, 2-8 to 2-22
- BOOTP servers, 2-6
- DHCP parameters, 3-7 to 3-8
- exceptions, 1-41
- RARP parameters, 4-3 to 4-5
- SNMP community members, 1-27 to 1-31
- threshold polling interval, 1-31
- thresholds, 1-31 to 1-39
- traps, 1-40 to 1-41

D

defaults
- for BOOTP and DHCP parameters, A-3 to A-4
- for RARP parameters, A-4
- for SNMP parameters, A-1

deleting
- BOOTP services, 2-22
- DHCP services, 3-8
- exceptions, 1-44
- RARP services, 4-8
- SNMP communities, 1-26
- SNMP managers, 1-31

DHCP
- implementation notes for, 3-6
- overview of protocol, 3-1
- packet, 2-5, 3-2 to 3-5
- servers, 3-1
- services, enabling, 3-6

DHCP parameters
- defaults, A-3 to A-4
- *See also* BOOTP parameters

DLCI Number parameter, 2-17

Dynamic Host Configuration Protocol. *See* DHCP

E

editing
- BOOTP parameters, 2-9 to 2-22
- DHCP parameters, 3-7 to 3-8
- managers, 1-29
- RARP parameters, 4-3 to 4-8
- SNMP community parameters, 1-24, 1-27
- SNMP global parameters, 1-21 to 1-23
- SNMP threshold parameters, 1-31 to 1-39
- SNMP trap parameters, 1-40 to 1-43

Enable parameter, for SNMP, 1-22

Enable/Disable parameter
- for BOOTP preferred server table, 2-20
- for BOOTP relay agent forwarding table, 2-14
- for BOOTP relay agent interface table, 2-10
- for RARP, 4-8

enabling
- BOOTP services, 2-7
- DHCP services, 3-6
- IP services, 1-16
- RARP services, 4-2
- SNMP services, 1-16

Entity Code parameter, 1-43

Ethernet History group, 1-4, 1-12

Ethernet Statistics group, 1-4, 1-11

Event Code parameter, 1-43

event messages, 1-8

exceptions
- configuring, 1-41
- deleting, 1-44

F

Filter group, 1-5, 1-15

filtering BOOTP and DHCP packets, 2-5, 2-6

H

History Control group, 1-4, 1-12

Hops parameter, 2-10

Host group, 1-4, 1-12

HostTopN group, 1-4, 1-13

I

implementation notes
- for BOOTP, 2-5 to 2-7
- for DHCP, 3-6
- for SNMP, 1-6 to 1-16

Input IP Address parameter, 2-13

interoperability issues for RMON, 1-10 to 1-16

IP
- address
  - acquiring through DHCP services, 3-1 to 3-5
  - acquiring through RARP services, 4-1
- configuration parameters, acquiring, 3-1
- parameters. *See* IP parameters

IP Address parameter
for BOOTP, 2-17
for IP, 1-19
for RARP, 4-7
IP parameters
IP Address, 1-19
Subnet Mask, 1-19
Transmit Bcast Addr, 1-19
UnNumbered Assoc Address, 1-20

L

Lock TimeOut parameter, 1-23

M

MAC Address, for RARP, 4-7
managers, for SNMP
adding, 1-27
deleting, 1-31
editing, 1-29
Matrix group, 1-5, 1-14
memory use
for configuring thresholds, 1-9
for RMON, 1-10 to 1-16

O

Output IP Address parameter, 2-14

P

packet
BOOTP, 2-1 to 2-4
filtering, 2-5, 2-6
DHCP, 3-2 to 3-5
filtering, 2-5, 2-6
Packet Capture group, 1-5, 1-15
parameters
See BOOTP parameters
See IP parameters
See RARP parameters
See SNMP parameters
Pass Through Mode parameter, 2-6
for BOOTP preferred server table, 2-21
for BOOTP relay agent forwarding table, 2-15
for BOOTP relay agent interface table, 2-11
Polling Interval parameter, 1-32

R

RARP
defining the mapping table for, 4-5
overview of protocol, 4-1
RARP parameters
defaults, A-4
Enable/Disable, 4-8
IP Address, 4-7
MAC Address, 4-7
Relay Agent IP Address parameter, 2-20
relay agent. *See* BOOTP
Remote network monitoring. *See* RMON
Request for Comments 1757, 1-2, 1-3
Reverse Address Resolution Protocol. *See* RARP
RIP, 1-20
RMON
agent, 1-3
control parameters, 1-3
control tables, 1-3
data tables, 1-3
groups, 1-3 to 1-5
interoperability issues, 1-10 to 1-16
memory use, 1-10 to 1-16
router mode, setting, 2-5

S

setting the router mode, 2-5
Simple Network Management Protocol
See SNMP
SNMP
applications or managers, 1-1
communities, 1-2
community
adding, 1-24

SNMP *continued*
deleting, 1-26
editing, 1-26
community members
configuring, 1-27 to 1-31
enabling, 1-16
implementation notes for, 1-6 to 1-16
network elements, 1-1
overview of protocol, 1-1
parameters. *See* SNMP parameters
security, 1-2
traps, 1-1, 1-9
SNMP parameters
accessing, 1-20
community
Access, 1-26
Community Name, 1-25
defaults, A-1
global
Authentication Failure Traps, 1-23
editing, 1-21 to 1-23
Enable, 1-22
Lock TimeOut, 1-23
Use Lock, 1-22
manager
Trap Port, 1-30
Trap Types, 1-30
threshold global
Polling Interval, 1-32
threshold interface
Threshold Action, 1-38
Threshold Enable, 1-35
Threshold High Event Level, 1-37
Threshold High Value, 1-36
Threshold HoldDown Intervals, 1-39
Threshold Label, 1-39
Threshold Low Event Level, 1-35
Threshold Low Value, 1-35
Threshold Max Successive Alarms, 1-38
Threshold Medium Event Level, 1-36
Threshold Medium Value, 1-36
Threshold Units, 1-37
trap interface
Always/Never Trap, 1-43
SNMP parameters *continued*
editing, 1-40 to 1-43
Entity Code, 1-43
Event Code, 1-43
specifying. *See* configuring, 2-22
Subnet Mask parameter, 1-19

T

Target Server IP Address parameter, 2-20
Threshold Action parameter, 1-38
Threshold Enable parameter, 1-35
Threshold High Event Level parameter, 1-37
Threshold High Value parameter, 1-36
Threshold HoldDown Intervals parameter, 1-39
Threshold Label parameter, 1-8, 1-39
Threshold Low Event Level parameter, 1-35
Threshold Low Value parameter, 1-35
Threshold Max Successive Alarms parameter, 1-38
Threshold Medium Event Level parameter, 1-36
Threshold Medium Value parameter, 1-36
threshold polling interval, configuring, 1-31
Threshold Units parameter, 1-37
thresholds, 1-6 to 1-9
configuring, 1-31 to 1-39
Timeout Secs. parameter, 2-11
Transmit Bcast Addr parameter, 1-19
Trap Port parameter, 1-30
Trap Types parameter, 1-30
traps, 1-1, 1-9
configuring, 1-40 to 1-41

U

UnNumbered Assoc Address parameter, 1-20
unnumbered interfaces, using for BOOTP and DHCP services, 2-7, 2-17
Use Lock parameter, 1-22